Nigeria Data Protection Act 2023: Key Regulatory Compliance Issues for Technology Companies

The Nigeria Data Protection Act, 2023 ("the Act") was signed into law on June 12, 2023 as the substantive legislation on data protection in Nigeria. While the Act presents substantial similarity with the Nigeria Data Protection Regulation, 2019 (NDPR) a pre-existing subsidiary regulation, it is remarkable in lending legislative force to the data protection framework in Nigeria and providing a statutory institution (Nigeria Data Protection Commission "Commission") with comprehensive enforcement and supervisory jurisdiction to strengthen the data protection regime in Nigeria. Notably, the Act preserves prior regulations on processing of personal data (such as the NDPR) but assumes ascendancy on all previous data protection regulations and such regulations shall continue to have effect only to the extent that they are consistent with the Act. In this article, we highlight key compliance issues especially for technology or technology-related companies.

General Framework for Data Collection, Use, Storage, Control and Processing.

Building on the NDPR groundwork, the Act defines a data controller as "an individual, private entity, public commission or agency or any other body who or which, alone or jointly with others, determines the purposes and means of the processing of personal data". A data processor on the other hand is defined as "an individual, private entity, public authority, or any other body, who or which processes personal data on behalf of or at the direction of a data controller or another data processor".
Resulting from the Internet of Things, technology operations typically collect, store, use and process significant volume of personal data- "information relating to an individual, who can be identified or is identifiable, directly or

indirectly, by reference to an identifier". Against this backdrop, the Act provides for the responsibility of the data controller or processor to ensure that personal data is processed in a fair, lawful and transparent manner; collected for specified legitimate purposes; adequate, relevant and limited to the minimum necessary, retained for no longer than necessary; accurate and complete; and processed in a manner that ensures appropriate security.

As data becomes an increasingly valuable asset, a commitment to ethical and legal data practices becomes a strategic imperative for sustainable growth in the technology sector.

Some Key Issues

Consent of Adults and Children
The primary lawful basis for the processing of personal data is first and foremost consent. The absence of consent takes the processing or controlling of personal data into the realm of illegality. It is important that a data subject's consent is obtained in a way that shows that it was freely and intentionally given as silence or inactivity will not constitute consent. The situation is however different for children and persons who lack the legal capacity to consent. Measures must be taken to verify the age of the data subject, and where it is a child or person lacking legal capacity, the consent of a parent or legal guardian must be obtained.

The right of consent also implies the right to withdraw consent to the processing of personal data. For this reason, the processes for withdrawal of consent must be as easy as the processes for giving consent. Technology firms that operate edtech and social networking for a user demography of persons below 18 years may have to undertake a compliance review of their user onboarding processes and privacy policies.

Higher Threshold of Security for Sensitive Personal Data

The Act imposes stricter responsibilities for the processing of sensitive personal data. Sensitive personal data include personal data relating to an individual's genetic and biometric data, race or ethnic origin, religious or similar beliefs, health status, sex life, political opinions or affiliations, trade union membership or other information prescribed as sensitive by the Commission.
A data processor or controller is not permitted to process sensitive personal data unless; the data subject has given consent for the specific purpose for which the data will be processed, it is necessary for the performance of certain obligations or exercising the data subject's rights under employment law, on a medical basis, for a public interest, it is necessary to protect the vital interests of the data subject and the processing is carried out in the course of its legitimate activities.

Additional Privacy Policy Requirements

The Act has now mandated that data controllers provide data subjects with its identity, residence or place of business, means of communication, specific lawful basis of processing, the purpose of the processing, recipients of the personal data, the existence of the rights of the data subject, retention period for the perusal data, right to lodge a complaint with the Commission and the existence of automated decision-making, including profiling. These must be contained in the privacy policy and must be expressed in a clear, concise, transparent, intelligible and easily accessible format.

Obligations when Engaging a Data Processor

A data controller or data processor engaging the services of another data processor must ensure that the engaged processor complies with its obligations under the act, respects the rights of data subjects and implements appropriate technical and organizational measures to ensure the security and confidentiality of personal data. This should be contained in the agreement between parties before the commencement of the business relationship.

Security and Breach of Data Privacy

Data controllers and data processors must implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its control or possession.

Measures to be taken include pseudonymization, encryption, restoration of data in the event of a physical or technical incident, periodic assessment of risks as well as regular testing and updates of adopted measures.

Notwithstanding the measures put in place, where a breach occurs, the data processor must timeously notify the data controller or data processor that engaged it. The Commission as well as the data subjects must also be notified depending on the degree of the breach and the likelihood of high risks to the rights and freedoms of the data subject. [3] Steps must then be taken to ensure timeous rectifications and restoration.

Cross-border Transfer of Personal data

Diverse technological operations require the seamless transfer and sharing of data across national borders. When a data controller or data processor engages in the cross-border transfer of personal data, either to another distinct entity or to its subsidiary, specific requirements govern these crucial data flows.

A fundamental condition is legal interoperability. The entity facilitating the cross-border data transfer must ensure that the recipient of the personal data is subject to laws, binding corporate rules, contractual provisions, a code of conduct, and certification processes that provide an adequate level of protection. A level of protection is deemed adequate if it is grounded in principles substantially similar to the conditions stipulated in the Act for the processing of personal data.

Additionally, the Nigerian-law subject must verify that the recipient entity adheres to robust data protection standards. This entails a thorough assessment of the recipient's corporate rules, security measures, encryption practices, and an overall commitment to maintaining the confidentiality and security of the transferred personal data, as disclosed in its policies and processes. In a few exceptions, a data controller or data processor may conduct cross-border data transfers without the adequacy of protection if the data subject has provided and not withdrawn consent, being duly informed of the potential risks associated with such transfers without adequate protections. Transfer, in the absence of protection adequacy, is also permissible under certain conditions:

·where the transfer is necessary for the performance of a contract to which a data subject is a party or to take steps at the request of a data subject, prior to entering into a contract,

·where the transfer is for the sole benefit of a data subject, and obtaining consent is not reasonably practicable or if it were reasonably practicable to obtain consent, the data subject would likely give it.

Further exceptions apply in cases where the transfer is justified by public interest, required for the exercise or defence of a claim, or necessary to protect the vital interests of a data subject or other persons. These exceptions also extend to situations where a data subject is physically or legally incapable of giving consent.

Concluding Remark

Ensuring data protection is essential for technology businesses, serving as both a regulatory compliance necessity and a best practice requirement within the operating ecosystem. Data processors or controllers failing to adhere to data protection standards that align with legal and regulatory requirements expose themselves to significant liability issues, impacting not only their own operations but also posing risks to other businesses engaged in data sharing or processing with them. The Nigeria Data Protection Act outlines extensive liabilities within both criminal and civil contexts for non-compliance. However, an equally compelling motivation for voluntary compliance stems from the imperative for firms to align with industry best practices to boost confidence in their data operations.

By maintaining data protection standards under the NDPA, technology businesses can effectively navigate the increasingly converging global data regulatory landscape. In doing so, they mitigate the risks associated with legal consequences and potential harm to their reputation. Non-compliance not only invites legal scrutiny but also jeopardizes the trust and confidence of stakeholders, including customers and partners. The NDPA, with its comprehensive framework, serves as a guide for businesses to establish and uphold data protection practices that meet or exceed regulatory requirements across several jurisdictions in which they and their affiliates and partners operate. As data becomes an increasingly valuable asset, a commitment to ethical and legal data practices becomes a strategic imperative for sustainable growth in the technology sector.

Data processors or controllers failing to adhere to data protection standards that align with legal and regulatory requirements expose themselves to significant liability issues, impacting not only their own operations but also posing risks to other businesses engaged in data sharing or processing with them. The Nigeria Data Protection Act outlines extensive liabilities within both criminal and civil contexts for non-compliance. However, an equally compelling motivation for voluntary compliance stems from the imperative for firms to align with industry best practices to boost confidence in their data operations.

Contributors

Abimbola Ojenike
abimbola@slingstonelaw.com

Damilola Omotosho
damilola@slingstonelaw.com