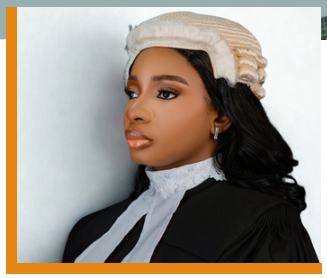
SYNTEGRAL
LEGAL PRACTICE

NDPA 2023 DEMYSTIFIED: ESSENTIAL COMPLIANCE REQUIREMENTS FOR NIGERIAN BUSINESSES

February, 2026



Tolulope Raji
Head, Capital Market



Igwebuike Ifunanya
Associate Counsel

The maxim ignorantia juris non excusat (ignorance of the law excuses no one) captures a foundational principle of legal order,compliance is not discretionary but obligatory. In contemporary digital economy, where personal data functions as both a commercial asset and an instrument of identity, regulatory oversight has become indispensable. The Nigeria Data Protection Act 2023 (the "Act") represents a significant legislative intervention aimed at institutionalizing accountability, transparency, and trust within Nigeria's rapidly evolving data ecosystem. It affirms that legal norms governing data processing are binding standards, not aspirational guidelines.

The Act establishes a comprehensive framework for the protection of personal data and creates the Nigerian Data Protection Commission (the "Commission") as the supervisory authority responsible for oversight and enforcement. In recognizing the intrinsic sensitivity of personal information and the potentially irreversible harm arising from its misuse, the Act seeks to safeguard the fundamental rights and freedoms of data subjects. It imposes defined obligations on data controllers[1] and data processors[2], mandates structured compliance mechanisms, and provides accessible avenues for redress in cases of infringement.

This article critically examines the statutory duties imposed on organizations under the Act, analyses the consequences of non-compliance, and advances practical recommendations for embedding sustainable data governance structures. In doing so, it situates compliance not merely as a legal burden, but as a governance imperative essential to institutional legitimacy, operational resilience, and long-term competitiveness in an increasingly data-driven marketplace.

1 A data controller is the organisation or person that decides why and how personal data is collected and used
2 A data processor is the organisation or person that handles personal data on behalf of the data controller, following the controller's instructions

KEY OBLIGATIONS OF ORGANIZATION UNDER NIGERIAN DATA PROTECTION ACT 2023

The Act stipulated critical obligations that every organization must comply with to safeguard the fundamental rights, freedoms and interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999. These obligations encompass lawful processing of personal data, protection of data subject rights, data security, regulatory registration, and reporting duties.

Lawful Processing: Under Section 24 (1) of the Act,organizations are required to process personal data lawfully, fairly, and transparently. Data must be collected for specific, explicit, and legitimate purposes and should not be used in a manner incompatible with these purposes. Organizations must limit data collection to what is necessary, ensure that information is accurate, complete, and up-to-date, and retain data only for as long as is required to fulfil its intended purpose.

Legal Obligations Towards Data Subjects[3]: Section 34 of the Act enshrines the rights of data subjects, and organizations have corresponding duties to uphold these rights. They must provide transparency regarding the processing of personal data, including details of purposes, categories of data, retention periods, recipients, sources, and any automated decision-making. Data subjects are entitled to access and portability of their information in commonly used electronic formats, and organizations must promptly correct or erase inaccurate or unnecessary data. Processing should be restricted where objections or review requests are raised, and organizations must maintain accessible complaint and redress mechanisms. Additionally, they are obliged to implement appropriate technical and organizational safeguards to protect personal data from unlawful access, loss, or destruction.

Data Security: Ensuring the security of personal data is a fundamental duty for all data controllers and processors. Organizations are required to implement robust technical and organizational measures that preserve data integrity, confidentiality, and system resilience. Security measures should be proportionate to the sensitivity of the data and the potential harm from breaches. Techniques such as pseudonymization[4], deidentification, and encryption should be employed where appropriate. Systems must be reliable, resilient, and capable of restoring access quickly following incidents, with risks evaluated regularly and security measures reviewed and updated to address emerging threats.

Appointment of a Data Protection Officer[5] (DPO): Major data controllers are mandated to designate a qualified DPO, who may be an internal employee or an external expert. The DPO is responsible for advising staff on lawful processing requirements, monitoring compliance with statutory obligations and internal policies, and acting as the primary contact with the Commission. This role ensures accountability and oversight for organisations handling significant volumes or sensitive categories of personal data.

3 Section 34-37 of the Nigerian Data Protection Act 2023.
4 Pseudonymization is simply a way of replacing identifying information with fake or coded details so a person can't be directly identified
5 A Data Protection Officer is a designated individual within an organisation who oversees how personal data is handled and ensures compliance with data protection laws

Registration and Fee Obligations[6] Organisations classified as data controllers or processors of major importance must register with the Commission within six months of attaining that status, providing details of their operations, categories of data processed, processing purposes, intended recipients, cross-border transfers, and safeguards in place. Significant changes must be reported within sixty days. Additionally, these entities are required to pay prescribed fees or levies as part of their regulatory compliance obligations.

Duty to Report Data Breaches: Section 40 of the Act obliges data processors to promptly notify controllers of any personal data breach. Controllers must report breaches likely to affect individual rights and freedoms to the Commission within seventy-two hours and, where high risk exists, inform affected data subjects directly or publicly. Notifications must detail the nature and consequences of the breach and the remedial measures undertaken. Organisations are required to maintain comprehensive records of all breaches, and the Commission retains the authority to issue regulations or make public statements where communications are inadequate.

PENALTIES FOR NON-COMPLIANCE WITH THE PROVISIONS OF Act 2023

Failure to comply with orders made under the Act constitutes a statutory offence applicable to both data controllers and data processors. Any organization or individual in breach of the Act's provisions is exposed to a range of sanctions, the severity of which depends on classification, culpability, and the nature of the contravention. Financial penalties are the primary enforcement mechanism. data controllers or data processors designated as being of Major Importance are subject to the higher statutory maximum fines prescribed under the Act. Entities not classified within this category remain liable to the applicable standard maximum penalties. The financial consequences may therefore be significant, particularly for organizations operating on a scale.

In addition to monetary sanctions, certain offences under the Act carry criminal liability. Upon conviction, a custodial sentence of up to one year may be imposed, depending on the nature and gravity of the breach. In appropriate circumstances, the court may order both a fine and a term of imprisonment, reflecting the seriousness of the violation. Beyond judicial sanctions, the Commission retains regulatory enforcement powers. These include the issuance of compliance and corrective orders, suspension of data processing activities, and the imposition of proportionate administrative fines. Such measures may be applied independently of, or alongside, court-imposed penalties

Other Risks of Non-Compliance

The consequences of non-compliance extend beyond formal sanctions. Reputational damage is often immediate and enduring. Regulatory findings or data breaches can significantly erode public trust, weaken brand integrity, and deter customers, partners, and investors from maintaining relationships with the organisation. Non-compliance may also result in exclusion from commercial opportunities. Many public procurement frameworks and private contractual arrangements require demonstrable data protection compliance as a condition of participation. Organisations that fail to meet statutory standards risk disqualification from tender processes or termination of existing agreement.

6 Section 44 - 45 of the Nigerian Data Protection Act 2023

BENEFITS OF COMPLIANCE

Conversely, compliance yields tangible institutional advantages. Adherence to statutory obligations fosters trust among customers and stakeholders by demonstrating a genuine commitment to safeguarding personal data. It enhances organisational credibility, signalling professionalism, regulatory alignment, and responsible governance. Operationally, compliance reduces the likelihood of disruptions arising from breaches, investigations, or enforcement actions. By embedding structured governance and risk controls, organisations are better positioned to maintain continuity and stability.

It is imperative to add that strong data protection compliance can confer a competitive advantage. Organisations that meet regulatory standards are more attractive to contracting authorities, commercial partners, and investors, particularly in sectors where data handling is integral to service delivery such as the telecommunication, fintech and electoral spaces.

PRATICABLE RECOMMENDATIONS

Embedding sustainable data governance within an organisation requires more than drafting policies or responding reactively to regulatory demands. It calls for deliberate institutional design, clear accountability, and a culture that recognises data protection as a core governance responsibility rather than a peripheral compliance task.

At the outset, data governance should be positioned firmly within the organisation's broader risk management framework. Boards and senior leadership must treat data protection as a strategic issue, with defined reporting lines linking the DPO, compliance teams, and IT security functions to executive decision-makers. Without visible commitment from the top, governance structures rarely achieve meaningful traction. The appointment of a suitably qualified and empowered DPO is equally important. The role should carry genuine authority, adequate resources, and direct access to senior management. A DPO who lacks independence or organisational influence cannot effectively oversee compliance or challenge high-risk processing decisions. For governance to endure, the role must be substantive rather than symbolic.

Clarity about data holdings is fundamental. Organisations should maintain an up-to-date record of the personal data they process, the lawful basis for doing so, how the data flows internally and across borders, how long it is retained, and which third parties are involved. Without a clear understanding of these elements, it is difficult to manage risk in a structured or defensible manner.Privacy considerations should also be embedded into operational processes from the outset. By adopting privacy-by-design[7] and privacy-by-default[8] principles, organisations ensure that data minimisation, access controls, security safeguards, and purpose limitation are integrated into systems and products at the development stage. This approach is far more sustainable than attempting to retrofit compliance after deployment.

7 Privacy by design means building privacy and data protection into a system, product, or process from the very beginning, rather than treating it as an afterthought. It requires that data protection safeguards be embedded into systems, products, and processes at the development stage, rather than applied retrospectively

8 Privacy by default means that the strictest privacy settings are automatically applied without requiring the user to take any action. It ensures that, by default, only the minimum personal data necessary for a specific purpose is processed, with the highest privacy settings automatically applied unless the user chooses otherwise.

Where processing activities present heightened risks such as those involving sensitive data, large-scale profiling, or emerging technologies Data Protection Impact Assessments[9] should be undertaken as a matter of course. This encourages thoughtful analysis of potential harms and ensures that mitigating measures are considered before risks materialise. Robust internal controls further reinforce governance arrangements. Policies relating to data protection, information security, breach management, retention, and vendor oversight should be practical, clearly communicated, and regularly reviewed. They must translate into consistent operational behaviour rather than remaining as static documents.

Third-party risk deserves particular attention. Many regulatory breaches arise through external processors or service providers. Careful due diligence, well-drafted data processing agreements, and ongoing monitoring are therefore essential components of a sustainable governance framework. Training and awareness also play a decisive role. Staff at all levels particularly those in human resources, IT, marketing, and management should receive periodic, role-specific training to ensure that data protection obligations are understood and applied in day-to-day activities. A well-informed workforce strengthens compliance far more effectively than written policies alone.

In addition, organisations should maintain a structured and tested incident response plan. Clear procedures for escalation, investigation, regulatory notification, and communication can significantly reduce the impact of a data breach and demonstrate regulatory accountability. Sustainable data governance requires continual review and refinement. Regular internal audits, monitoring of regulatory developments, and iterative improvements help ensure that governance arrangements remain aligned with legal standards and organisational growth.

Ultimately, sustainable data governance is best regarded as an ongoing governance discipline rather than a one-off compliance exercise. Organisations that approach it in this way are better placed to safeguard trust, manage risk responsibly, and operate with credibility in an increasingly data-driven economy.

9 A Data Protection Impact Assessment is a structured process used to identify, assess, and minimise risks to individuals' personal data before starting a high-risk processing activity.

CONCLUSION

Compliance with the Act is not merely a statutory requirement; it is a critical component of sound corporate governance and strategic business practice. Beyond the avoidance of regulatory sanctions, compliance demands the embedding of accountability[10], transparency, and operational resilience into the very fabric of organisational systems and culture. By adhering to the provisions of the Act, data controllers and processors not only protect the rights and freedoms of data subjects but also strengthen institutional credibility, governance standards, and reputational capital.

To build a sustainable data governance and compliance framework, organisations must prioritize the appointment of competent and independent Data Protection Officers, ensure timely registration and engagement with the Commission, and implement comprehensive technical and organisational security measures. Effective governance also requires the development of robust data breach detection and response protocols, ongoing compliance monitoring, periodic reviews of data protection safeguards, and proactive, transparent communication with both regulators and data subjects. In doing so, organisations transform compliance from a legal obligation into a strategic enabler one that reinforces trust, supports operational resilience, and positions the business to compete responsibly in an increasingly data-driven economy.

10 NDPC Guidance Notices https://www.ndpc.gov.ng/ Accessed 31st January 2026.

©Syntegral Legal Practice

+234 802 575 4547
info@syntegralp.com
@syntegral_lp