Analysis of Nigeria's Data Protection Law

budgIT

1

Background and Introduction

The Nigeria Data Protection Act (NDPA) was signed into law in June 2023, and came into full effect from September 2025. Since then, the current NDPA framework has replaced the previous Nigeria Data Protection Regulation (NDPR) to advance a trusted digital economy amid rising data volumes and AI-driven risks.

2

Strengthening Data Privacy Rights

- The General Application and Implementation Directive (GAID) enforces constitutional privacy rights under Section 37 of the 1999 Constitution.
- Every citizen, whether in Nigeria or abroad, has the right to data protection.
- The directive emphasises that privacy is a fundamental human right, not a privilege.

3

Clarity on Who Must Comply

- All data controllers and processors in Nigeria, as well as those outside Nigeria that process data of Nigerian citizens, are required to comply.

- The Act categorises organisations into Ultra-High, Extra-High, and Ordinary-High Levels depending on their data volume and sensitivity.

4

Mandatory Compliance Requirements

- Register with the Data Protection Commission (NDPC).
- Conduct annual audits and file Compliance Audit Returns (CAR).
- Appoint a Data Protection Officer (DPO) and file semi-annual reports.
- Notify the Commission of any data breaches within 72 hours.
- Conduct Data Privacy Impact Assessments (DPIAs) for high-risk or large-scale data processing activities.

5

Accountability and Enforcement

- Non-compliance attracts administrative penalties and may result in the restriction of operations.
- The Commission has complete jurisdiction to ensure transparency, proportionality, and lawfulness in the processing of data.

6

Data Ethics and Emerging Technologies

- GAID introduces new standards for ethical AI, cookies, tracking tools, and cross-border data transfers.
- Organisations must ensure that privacy is built into all technology deployments.

7

Collaboration and Capacity Building

- The NDPC will partner with public institutions to establish Data Privacy Service Units and Centres of Excellence.

- Continuous training and certification for DPOs are now mandatory.

Key Rights and Obligations for Citizens

These are the powers and responsibilities that the law grants to individuals, along with the actions that citizens must take to benefit from those rights.

Right/Obligation	What It Means	How Citizens Can Use / Do It
Right to be informed	Citizens must be told by organisations what personal data is being collected, why, who will use it, and for how long.	Read privacy notices and terms & conditions; ask organisations for this information.
Right of access	Citizens can request and get a copy of their data held by controllers/processors.	Submit access requests to organisations; use NDPC if denied.
Right of rectification	Ability to correct wrong/incomplete personal data.	Monitor your profile information (e.g., banks, telecom) and notify us of any errors.
Right to erasure, i.e. right to be forgotten	Citizens can ask organisations to delete data that's no longer needed or processed unlawfully.	Use deletion requests; follow up if no response.
Right to restrict processing/object	Individuals can restrict how their data is used (especially for marketing, profiling, etc.) or object to specific uses.	Opt out of non-essential data processing; opt in only where necessary.
Right to portability	You can receive your data in a machine-readable format and transfer it to another location.	Request downloadable copies of data (e.g., account transfer information).
Right not to be subject to automated decision-making	When decisions are made solely by automated systems (without human input), citizens have the right to challenge or request human review.	If denied a job, loan, service, or other benefit by an automated system, request an explanation or human review.

budgIT

Critical Gaps/Issues in Data Protection Compliance

- **Many organisations lack visible privacy notices** or have policies that are hard for citizens to find.
- **Low awareness** among citizens of their rights (access, erasure, portability).
- **Organisations delaying compliance:** delaying registration, DPO appointment, or audit returns.
- **Technical capacity gap:** Many entities struggle to implement breach-reporting and DPIAs correctly or at all.
- **Enforcement is recent and growing** – but compliance in both the public sector and private sector is patchy.

The Nigerian Data Protection Laws provide clear and enforceable obligations on all parties, including citizens, the public, and the private sector. The citizens gain stronger rights, where private/public institutions must comply with registration, security, transparency, and breach response requirements. Empirical enforcement is underway, yet there is a significant gap in timely awareness, which is a key challenge for data protection compliance among players.

budgIT

budgIT

Check out our latest chatbot

www.bimi.budgit.org