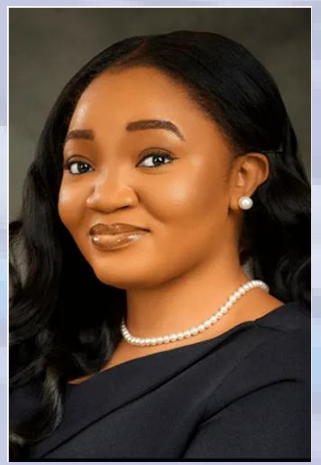
DEAR TECH BRO/SIS, BEFORE YOU LAUNCH THAT APP, LET'S TALK DATA PROTECTION!

Yinka Edu
Partner



Chisom Okolie
Senior Associate

Opeyemi Adeshina
Associate

Joel Adefidipe
Associate

u-law @ulawsocial

You and your team are about to launch the next big thing in tech, possibly the iPhone moment of the African startup scene. Your product is a bona fide disruptor. You are already beta testing, running surveys and gathering valuable personal data from test users.
But pause for a second. Have you really considered the data protection angle of your operations?

In Nigeria, data protection has evolved far beyond a simple compliance checkbox. The Nigeria Data Protection Commission ("NDPC") has shifted from simply encouraging compliance to actively enforcing the law and issuing penalties for non-compliance. The last thing you want is for your startup to go viral for the wrong reasons, like being flagged for a data breach before your product takes off.

This article is the insider guide you didn't know you needed - clear, practical, and founder-friendly. We take you through how to stay compliant, build user trust, and launch your product without legal "baggage".

Get Started

Subscribe to our mailing list u-law ulawsocial

WHAT YOU NEED TO KNOW

1 **Know the Law:** In Nigeria, the principal legislation governing data protection is the Nigeria Data Protection Act, 2023 (“NDPA”). On 20 March 2025, the Nigeria Data Protection Commission (“NDPC”) issued the General Application and Implementation Directive, 2025 (“GAID”), which took effect on 19 September 2025. The GAID now serves as the primary guidance for implementing the NDPA. There may also be sector-specific regulations you need to be aware of depending on the sector you operate in. Seek guidance early to see if any other laws are applicable to your business.

2 **Get Consent Right:** Where consent is the legal basis for processing personal data you collect, it must be freely given, specific, informed, and unambiguous. Your users need to know exactly what they’re agreeing to, and they must say “yes”; silence doesn’t count! Clearly explain why you need users’ data and avoid coercion or manipulation. Make it easy for users to withdraw consent at any time and let them know they can do so. For children’s data, ensure you implement an age gate and get verifiable consent from a parent or legal guardian.

3 **Protect Your Users’ Personal Data:** Lack of firewalls, encryption, 2FA authentication, antivirus, or access policy signals poor security. The NDPA legally requires technical and organisational measures to keep personal data secure. Prevent leaks or breaches by installing firewalls, restricting access, encrypting data, enforcing data protection policies, and training staff in security best practices.

4 **Cross-Border Data Transfers:** The NDPA regulates the transfer of personal data across borders. Section 41 permits such transfers only where the recipient is subject to a law or framework comparable to the NDPA, including Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), Codes of Conduct (CCs), or Certification Mechanisms (CMs). Section 43 provides that if such laws are absent, transfers require consent, unless it is necessary for a contract or public interest, for legal claims, to protect vital interests, or for the data subject’s benefit. The GAID clarifies that Nigerian organisations must use SCCs,

BCRs, CCs, or CMs unless the NDPC specifically designates a country as adequate. Since no designation has been given so far, you should use suitable transfer mechanisms and, if necessary, submit these to the NDPC for approval prior to implementation.

5 **Implement Organisational Policies:** Protect your users and your business by having clear data protection policies. Start with a Privacy Policy that explains how you collect, use, and store data, and allows users to exercise their rights. Internally, prepare and implement a Data Protection Policy that defines roles, responsibilities, and safeguards personal data. Establish a Data Protection Impact Assessment (DPIA) policy to identify and address privacy risks in new projects. A Data Breach Policy is also essential, so you are prepared to respond quickly and diligently to security incidents.

6 **Prepare for Data Breaches:** Have a Data Breach Policy to ensure an organised response. The NDPA requires that breaches be reported to the NDPC within 72 hours if the rights of data subjects are at risk. Affected individuals must also be notified promptly.

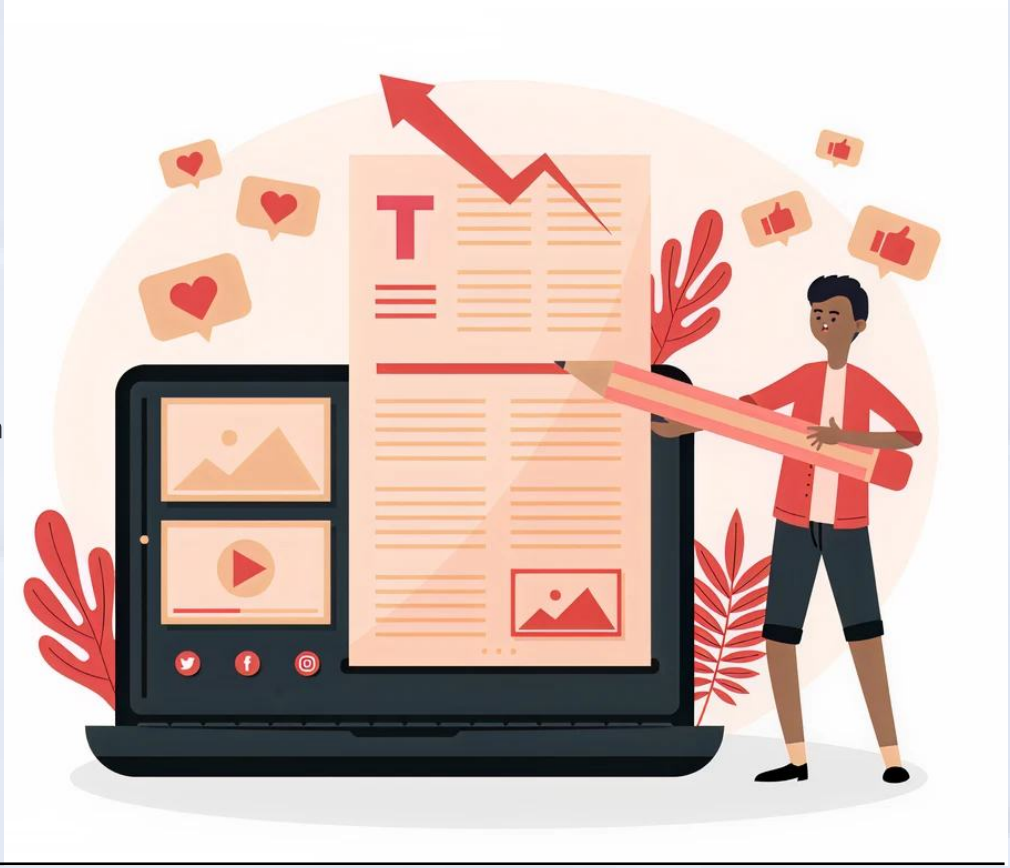
When evaluating the risk, factors like the effectiveness of mitigation measures (e.g., encryption), the nature of the data, and its sensitivity should be considered. Any data breach must be addressed within one month, and records of the breach, including facts, effects, and corrective actions, must be kept by a Data Protection Officer or an appropriate employee.

7 **Annual Audit:** Data protection audits in Nigeria are crucial for ensuring compliance with the NDPA and safeguarding personal data. These audits assess how organisations handle personal data to identify gaps in compliance and ensure it aligns with legal requirements. Organisations are required to engage a Data Protection Compliance Officer ("DPCO") to oversee the audit process, and the resulting report recommends corrective actions. Regular audits help prevent penalties and build customer trust. If required by law, the DPCO files the audit report to the NDPC.

CONCLUSION

So, dear founder, as you fine-tune your product, ensure it's not only sleek and functional, but also fully compliant before you hit the launch button. In Nigeria's current regulatory climate, overlooking data protection is a direct route to fines, reputational damage, and eroding the trust you've worked so hard to build with users. With the NDPA now in full swing and with enforcement intensifying, taking data privacy seriously isn't optional; it's survival.

If you are building or launching a product that processes personal data and you need guidance on your obligations under the NDPA, or want to ensure your startup stays compliant, or if you require any other information with respect to data protection or our broader practice area offerings, please contact us at: ulawteam@uubo.org or dpteam@uubo.org



Disclaimer

This update is for general information and does not constitute legal or tax advice. UUBO has an active tax team and is available to provide any assistance or clarification that you may require on how this update could apply to you or your business or on any matter. Any questions on this or other enquiries can be directed to your usual UUBO contact or to CorpTaxTeam@uubo.org