LEAP WISE LP

Nigeria Data Protection Act 2023: What Startups Actually Need to Comply With

November 14, 2026 · By Rory Ovedje, Esq. & Michael Adetunji · 8 min read

Nigeria Data Protection Act 2023: What Startups Actually Need to Comply With

Most founders fall into one of two camps on data protection. Either they assume the law is for banks and telcos, not a startup with a few thousand users — or they assume every startup needs a full compliance programme from day one and either do nothing because it feels overwhelming, or spend money on obligations that don't actually apply to them yet.

Neither assumption is reliable. The Nigeria Data Protection Act 2023 (NDPA) applies based on specific thresholds, and the honest first step is working out where your business actually sits — not guessing.

The direct answer

The NDPA applies to any organisation, in Nigeria or abroad, that processes the personal data of individuals in Nigeria. Every business that handles personal data has baseline obligations under the Act. But a specific, more demanding set of obligations is the mandated registration with the Nigeria Data Protection Commission (NDPC), appointment of a data protection officer, and filing of annual compliance returns. All these apply specifically to organisations classified as a Data Controller or Data Processor of Major Importance (DCPMI). Whether your startup falls into that category depends on defined thresholds, not the size of the company generally.

Who counts as a Data Controller or Processor of "Major Importance"

The NDPC's NDPA General Application and Implementation Directive as well as the Nigerian Data Protection Act sets out several ways a business can be classified as an entity of major importance, including:

- Processing personal data of more than 200 data subjects within a six-month period
- Operating in specific sectors the NDPC treats as higher-risk, including finance, health, insurance, communications, education, oil and gas, aviation, and tourism
- Providing digital services — including cloud storage or communication tools — that run on other people's devices
- Holding a fiduciary-type relationship involving personal data, such as guardianship-type arrangements
- Processing sensitive personal data considered important to Nigeria's economy or national security

This matters because the threshold isn't about company size or funding stage. A small fintech app with a few thousand users can clear the 200-data-subject threshold within its first few months of operation, while a much larger company processing data in a lower-risk way might not trigger the same obligations. The only way to know is to actually check against the thresholds, not assume based on how "big" the business feels.

What every business handling personal data must do, regardless of classification

Even startups that don't meet the "major importance" threshold have baseline obligations under the NDPA — this isn't optional just because you're small. These generally include having a lawful basis for processing personal data (typically consent, or another recognised legal basis such as contractual necessity), being transparent with users about what data is collected and why, and only processing data for the purposes it was actually collected for.

What Data Controllers and Processors of Major Importance must additionally do

If your startup meets the threshold, the obligations step up meaningfully:

Register with the Nigerian Data Protection Comission(NDPC). The NDPA requires registration within a set window after the Act's commencement, or within a set window after your business becomes a DCPMI, whichever applies. The NDPC has published guidance on how registration works, including categorising registered entities by processing scale. Registration deadlines and requirements have shifted since the Act came into force as the NDPC has issued further guidance, so this is an area to check against the NDPC's current published position rather than assume based on older information.

Designate a Data Protection Officer (DPO). A DCPMI must appoint someone with the expertise to advise on compliance, monitor internal practices, and act as the point of contact with the NDPC. For an early-stage startup, this doesn't necessarily mean a full-time hire — it can be a designated existing team member or an outsourced arrangement — but the role needs to exist and be properly documented.

Notify the NDPC of qualifying breaches, and affected individuals where there's high risk. The NDPA requires breach notification to the NDPC within a defined short window (72 hours) of becoming aware of a breach likely to pose a high risk, along with notifying affected individuals where the risk to them is high.

Keep records of processing activity. This means maintaining documentation of what personal data is collected, why, how it's stored, and who it's shared with — not just having good practices informally, but being able to demonstrate them.

File an annual compliance return. DCPMIs are required to file periodic compliance audit returns with the NDPC, generally on an annual basis, through a licensed Data Protection Compliance Organisation. Exact deadlines have moved before and are worth confirming against the NDPC's current notices rather than a fixed date, since the Commission has extended filing windows in the past.

What non-compliance actually costs

The NDPA sets tiered penalties depending on the size and classification of the organisation — generally structured as a fixed naira amount or a percentage of annual gross revenue, whichever is higher, with the higher tier applying to data controllers and processors of major importance. Beyond direct fines, the NDPC has demonstrated it will enforce actively, including significant penalties against major organisations such as Meta, and non-compliance with NDPC orders can also carry the risk of imprisonment for individuals responsible. Late registration and late filing of compliance returns can also attract separate surcharges.

For a startup, the more immediate commercial risk is usually not the fine itself — it's what an unresolved compliance gap does during an investor's due diligence process, or the cost and disruption of scrambling to register and document practices retroactively once the NDPC has already flagged the business.

Why investors specifically ask about this

Data protection compliance has become a standard diligence question for investors in fintech, healthtech, e-commerce, and any data-driven product, for two reasons. First, it's a direct regulatory and financial risk to the business they're investing in. Second, how a founder answers the question — a clear, considered position versus "we haven't really looked into it" — signals something broader about how carefully the business is being run.

An honest "we don't currently meet the major importance threshold, and here's why" is a perfectly good answer to an investor. "We haven't checked" is not.

A practical self-assessment

Work through this before assuming either way:

- Do you process personal data of more than 200 individuals within any six-month period?
- Does your business operate in a sector the NDPC treats as higher-risk — finance, health, insurance, communications, education, and similar categories?
- Do you provide a digital service that runs on other people's devices, such as cloud storage, messaging, or similar tools?
- Do you process any category of sensitive personal data at a meaningful scale?
- If any of the above applies: have you registered with the NDPC, designated a data protection officer, and do you have a documented breach response process?

If you're unsure about more than one of these, that uncertainty is itself the gap worth resolving — not the specific answer to any single question.

Common mistakes startups make

Assuming the law doesn't apply because the company is small. The thresholds are based on data processing activity and sector, not company size or funding stage.

Treating compliance as a one-time task rather than an ongoing obligation. Registration and an initial policy don't satisfy the requirement — annual compliance returns, updated records of

processing, and breach-readiness are ongoing responsibilities.

Not revisiting the assessment as the business grows. A company that didn't meet the 200-data-subject threshold at launch can cross it well before its next funding round, without anyone deliberately checking.

When to get professional help

Determining whether your business meets the major importance thresholds, and if so, properly registering and documenting compliance, is detailed regulatory work that benefits from a proper legal assessment rather than a best guess. Given how actively the NDPC has been enforcing, and how directly investors now ask about this, an unclear answer is a real gap, not a neutral one.

Where Leap Wise fits

Data protection compliance is increasingly a standard item in investor due diligence for Nigerian tech startups, and it's one of the easier gaps to resolve proactively — but only if it's actually assessed rather than assumed. If you are preparing for fundraising, Leap Wise LP can review your corporate, contractual and compliance position — including your position under the Nigeria Data Protection Act 2023 — and identify issues that may surface during investor due diligence.

FAQ

Does a small startup with a few hundred users need to worry about the NDPA? It depends on whether you're likely to cross the 200-data-subject threshold within a six-month period, and whether you operate in one of the higher-risk sectors the NDPC specifically flags. This is worth actually checking rather than assuming either way.

What happens if I've never registered and I've crossed the threshold? Late registration generally attracts a penalty, though the NDPC has previously allowed waivers in some circumstances, such as for newly incorporated entities. The right approach is to register properly as soon as the gap is identified, rather than continuing to operate unregistered.

Do I need a full-time Data Protection Officer as a small startup? Not necessarily a dedicated full-time hire — the role can often be filled by an existing team member with the right training, or through an outsourced arrangement — but the appointment needs to be real, documented, and the person needs to actually understand the compliance obligations they're responsible for.

How often do NDPC's rules and deadlines change? More frequently than founders expect. The NDPC has issued further guidance and adjusted filing deadlines since the Act came into force, so treat specific dates as things to verify against the NDPC's current published notices rather than fixed points.

Read online: https://leapwiselp.com/blog/nigeria-data-protection-act-2023-what-startups-actually-need-to-comply-with
© Leap Wise LP. Move boldly. Move wisely.