TRELLIS AFRICA

The NDPA Compliance Checklist

Ten questions every Nigerian startup should be able to answer about its data practices.

The Nigeria Data Protection Act 2023 (NDPA) is the law that governs how your company collects, stores, and uses personal data, and it applies whether you are a five-person startup or a listed bank. This checklist is not a substitute for a full data audit, but it is a fast, honest way to find out where your gaps are before a regulator, an investor's legal team, or a customer's complaint finds them for you.

Work through each question. If you cannot answer it clearly, that is your starting point.

01

1. Do you know exactly what personal data you collect, and why?

Why it matters: The NDPA requires a lawful basis and a stated purpose for every category of personal data you process. Vague or evolving justifications are the first thing a regulator or investor's counsel will probe.

A compliant answer looks like: You can list, in one document, every category of personal data you collect (names, emails, phone numbers, transaction data, location data, biometric data, etc.) and the specific business reason for each.

02

2. Do you have a lawful basis for each category of processing?

Why it matters: Section 25 of the NDPA sets out the only bases on which processing is lawful: consent, contract performance, legal obligation, vital interests, public interest, or legitimate interest. Relying on none of these, or misapplying one, exposes you to enforcement.

A compliant answer looks like: Each processing activity in your data map is tagged with one of the six lawful bases, and that basis is defensible if questioned.

03

3. Is your consent mechanism actually valid?

Why it matters: Where you rely on consent, the NDPA requires it to be specific, informed, freely given, and unambiguous. Pre-ticked boxes, bundled consent, or consent buried in a general terms-of-service click-through will not hold up.

A compliant answer looks like: Consent is captured through a clear affirmative action, tied to a specific purpose, and the data subject can withdraw it as easily as they gave it.

04

4. Do you have a privacy policy that reflects what you actually do?

Why it matters: A privacy policy copied from a template or another company's website, without matching your real data practices, is worse than having none. It is a written record the NDPC can hold you to.

A compliant answer looks like: Your privacy policy is written in plain language, names your actual data categories and purposes, discloses any third-party sharing, and states how long you retain data.

05

5. Do you have a Data Protection Officer, or do you need one?

Why it matters: Data controllers of major importance must designate a Data Protection Officer with expert knowledge of data protection law. Under the NDPC's General Application and Implementation Directive, this threshold is triggered by processing personal data of

more than 200 data subjects in six months, operating in specified sectors, or providing ICT services on devices holding others' data.

A compliant answer looks like: You have assessed whether you meet the major importance threshold, and either designated a DPO or documented why one is not yet required.

06

6. If you share data with vendors or partners, is there a written data processing agreement?

Why it matters: The NDPA requires a written agreement between a data controller and any data processor it engages, setting out security measures and compliance obligations. An informal understanding with your cloud provider or CRM vendor does not satisfy this.

A compliant answer looks like: Every third party that processes personal data on your behalf, payment processors, email platforms, analytics tools, is covered by a signed data processing agreement.

07

7. Do you have a plan for a data breach, before one happens?

Why it matters: Breach notification obligations under the NDPA run on a short clock. Figuring out your response process while a breach is unfolding costs you time you do not have and increases regulatory and reputational exposure.

A compliant answer looks like: You have a written breach response protocol, know who is responsible for assessing and notifying the Nigeria Data Protection Commission, and understand the applicable notification timeline.

08

8. If you transfer data outside Nigeria, have you documented the basis for that transfer?

Why it matters: Cross-border transfer of personal data is only lawful where the destination offers adequate protection, appropriate safeguards exist, or another recognised basis applies. Many early-stage companies transfer data internationally by default, through cloud hosting or foreign SaaS tools, without ever considering this.

A compliant answer looks like: You know where your data physically sits, and you can point to the specific legal basis that makes each cross-border transfer lawful.

09

9. Can a data subject exercise their rights if they ask you to?

Why it matters: The NDPA gives individuals the right to access, correct, delete, and port their data, and to object to certain processing. If a customer emails asking you to delete their account today, you need a process, not a scramble.

A compliant answer looks like: You have a defined internal process for handling data subject requests, with a clear owner and a realistic response timeline.

10

10. Do you actually know if you are a controller of major importance, and what that means for you?

Why it matters: This single classification determines whether you need to register with the NDPC, appoint a DPO, and file annual compliance audit returns. Getting it wrong in either direction, assuming you are exempt when you are not, or over-engineering compliance you do not yet need, both carry costs.

A compliant answer looks like: You have made a documented, deliberate assessment of your major importance status, rather than an assumption.

WHAT TO DO WITH THIS

If you answered most of these confidently, your next step is formalising what you already do into written policy, so it holds up under scrutiny rather than living in your head.

If several of these exposed a gap, that is normal for an early-stage company, and it is fixable. Trellis Africa runs a full data audit and NDPA compliance build for early-stage companies, covering everything from your privacy policy to your data processing agreements to your breach response protocol.

Talk to Trellis about your NDPA compliance build → hello@trellis.sbs