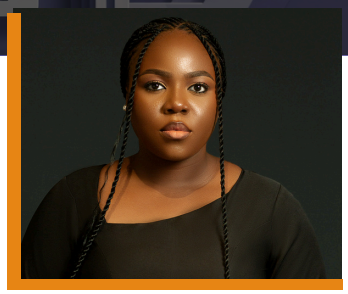
# DATA PROTECTION IN NIGERIA: WHO NEEDS AN NDPC AUDIT AND WHY THE TRUST MARK MATTERS.

January, 2026



Oladiran Falore
Managing Partner



Precious Bassey
Associate Counsel

The Nigerian data privacy landscape has experienced a transformative shift with the enactment of the Nigeria Data Protection Act (NDPA) 2023 and the establishment of the Nigeria Data Protection Commission (NDPC) as the country's primary regulatory authority. The NDPC has since taken a proactive stance on compliance, conducting sector-wide investigations and issuing formal notices to ensure organizations adhere to statutory requirements. Against this backdrop, the concept of an "annual audit" has evolved from a recommended best practice to a mandatory statutory obligation for thousands of organizations. A cornerstone of this compliance framework is the Audit Trust Mark, introduced by the NDPC as a key mechanism to demonstrate regulatory alignment and organizational accountability.

The Audit Trust Mark is a way for organizations to show they handle personal data responsibly and transparently. But who exactly needs to go through an NDPC audit? Which types of businesses are affected? This article looks at the entities caught by the regulations and explains why the Trust Mark has quickly become a key measure of credibility and trust in Nigeria's digital economy.

## WHAT IS THE NDPC AUDIT TRUST MARK?

The NDPC Audit Trust Mark is an official compliance recognition issued following a successful data protection audit. It confirms that an organization has conducted a valid NDPC compliant audit, met the minimum statutory and regulatory data protection standards, has implemented appropriate technical and organizationalsafeguards and is subject to ongoing regulatory oversight. The Trust Mark functions as both a regulatory compliance indicator and a market-facing credibility signal.

The NDPC derives its audit and enforcement powers primarily from The Nigeria Data Protection Act, 2023 as well as the NDPC Regulations, Guidelines, Implementation Frameworks and also Sector-specific data protection obligations imposed on regulated entities. Under the NDPA, data controllers and data processors are required to demonstrate compliance, not merely claim it. Periodic data protection audits conducted through NDPC licensed Data Protection Compliance Organizations (DPCOs) form a core part of this accountability framework.

A central component of this enforcement regime is the Compliance Audit Return and the subsequent issuance of the Audit Trust Mark. For many boards and C-suite executives, the question is no longer "should we comply?" but rather "are we legally required to file, and what is the strategic value of the Trust Mark?"

**WHO NEEDS AN NDPC AUDIT?**

The requirement to conduct a Data Protection Compliance Audit and file a Compliance Audit Report depends on the volume of data processed and the nature of an organization's operations. While all entities handling personal data in Nigeria have compliance obligations, the NDPC applies a risk- and category-based approach to determine audit intensity.

**1. Numerical Threshold**

Any Data Controller or Data Processor handling the personal data of more than 2,000 data subjects within 12 months must file an annual audit report. "Data subjects" include employees, contractors, vendors, visitors, and individuals captured on CCTV.

**2. Data Controllers and Processors of Major Importance**

Certain organizations are categorized as "Major Importance" due to the sensitivity of the data they handle or their economic impact. These groups are subject to stricter oversight:

• Major Data Processing – Ultra High Level: The largest entities whose data activities have systemic importance, including commercial banks, telecommunications companies, insurance firms, and multinational corporations handling data of over 5,000 subjects in 6 months. They process highly sensitive personal data, engage in cross-border transfers, and often rely on third-party cloud services.

• Major Data Processing – Extra High Level: Large public and private organizations with sensitive data, such as MDAs, microfinance banks, universities, mortgage banks, and secondary/tertiary hospitals. These entities process over 1,000 data subjects in 6 months and are expected to maintain high accountability and global best practices.

• Major Data Processing – Ordinary High Level: Smaller entities that still require formal oversight, including SMEs handling sensitive data, primary/secondary schools, clinics, independent labs, and small hotels (under 50 suites). These process over 200 data subjects in 6 months and must implement technical and organizational measures aligned with best practices.

**3. Discretionary Designation by the NDPC**
The NDPC may designate any organization for audit based on risk assessments, complaints, data breaches, or sector-wide compliance reviews, even if the organization does not fall within a high-risk category.

**WHY THE NDPC AUDIT TRUST MARK MATTERS**
While some critics argue that the Trust Mark represents "procedural" rather than "substantive" compliance, its value in the current Nigerian market cannot be overstated. The Trust Mark serves as a formal attestation from the NDPC that an organization has fulfilled its statutory filing obligations. In the event of a data breach, having a valid Trust Mark provides evidence of accountability, demonstrating to the regulator that proactive steps were taken to assess and manage data protection risks, which can significantly mitigate the severity of penalties.

As awareness of data privacy grows among Nigerian consumers, the Trust Mark has become a "badge of honor." It enhances business-to-business trust, as large multinationals and government agencies increasingly require proof of NDPC compliance and the Trust Mark before onboarding new vendors. Displaying the Trust Mark on websites and marketing materials signals to customers that their personal information is handled by an organization under regulatory oversight, thereby boosting consumer confidence.

In certain sectors, evidence of NDPC audit compliance is becoming a prerequisite for licensing, partnerships, and government contracts. Regulated industries such as financial services, telecoms, and digital platforms are particularly affected. Compliant organizations are typically listed on the NDPC's website, which serves as a public database often consulted by investors, auditors, and international partners performing due diligence on Nigerian entities.

**CONSEQUENCES OF NON-COMPLIANCE**
Failure to conduct NDPC-required audits or obtain a Trust Mark carries significant consequences, including financial penalties under the NDPA, enforcement actions, suspension of data processing, reputational damage, and potential loss of business opportunities. Non-compliance is no longer a low-risk option.

In Nigeria's evolving data protection landscape, audit readiness is increasingly synonymous with regulatory credibility. The Trust Mark is not a one-time exercise but a continuous governance commitment. Organizations that embed data protection into their operations and risk frameworks are better positioned to meet regulatory expectations, reduce enforcement exposure, and build trust with customers, partners, and regulators. For entities handling high-risk, high-impact, or sensitive data, audits must be treated as a mandatory governance obligation rather than an optional exercise.

## CONCLUSION

A Data Protection Compliance Audit must be facilitated by a Data Protection Compliance Organization (DPCO)which comprise of professional entities such as law firms, IT consultancies, or audit firms licensed by the NDPC. Beyond compliance, the NDPC audit serves as a diagnostic tool, helping organizations identify vulnerabilities before they result in costly breaches, and has become a central pillar of Nigeria's data protection framework. For any organization processing the personal data of over 2,000 Nigerians, or operating within the "Major Importance" categories, engaging a DPCO without delay is critical. Failure to secure the Data Protection Audit Trust Mark not only attracts regulatory fines but also signals a lack of transparency, potentially eroding customer trust in a digital-first economy. Organizations that act early can reduce regulatory risk while positioning themselves as credible, trustworthy custodians of personal data in an increasingly compliance-conscious environment.

## REFERENCES


• AUN Journal. (2025). *Data privacy and consumer protection in Nigeria's digital economy. AUN Journal of International Law*, 5(1).
• Chukwuemeka Odumegwu Ojukwu University. (2025). *An appraisal of the legal framework for tech giants in Nigeria. COOU Journal of Private and Public Law*, 7(2).
• Enwere, C. J., & Okobia, I. M. (2025). *Key provisions of the Nigerian Data Protection Act, 2023. Preorc Journal of Arts and Humanities*, 9(1).
• Nigeria Data Protection Act, 2023.
• Nnamdi Azikiwe University. (2025). *Corporate responsibility and data privacy legal obligations. Preorc Journal of Law and Jurisprudence*, 1(1).
• University of Cape Coast. (2025). A critical analysis of the Nigeria Data Protection Act 2023. UCC Law Journal, 4(2).


## EDITORS NOTE

**This article reflects the Nigerian data protection law and regulatory guidance as at the date of publication. Regulatory interpretations and enforcement priorities may evolve, and professional advice should be sought for specific compliance obligations.**