

September, 2025

SYNTEGRAL LEGAL PRACTICE

DOCUMENTS IN THE OPEN: NAVIGATING PRIVACY IN NIGERIA'S PUBLIC RECORDS

Authors



Tolulope Raji
Head, Capital Market



Precious Orowa
Senior Associate



Ifunanya Igwebuike
Associate Counsel

ABSTRACT

Recent headlines revealed how a politician's tax certificate, a government-issued document, became public fodder and sparked serious questions about privacy. This article examines whether sensitive records such as tax clearances can be freely circulated once they are classified as public documents under Nigerian law. The Evidence Act defines what constitutes a public document, while the Freedom of Information Act guarantees access to official records but explicitly exempt personal data from disclosure. The Nigeria Data Protection Act 2023 further strengthens privacy by requiring any processing of personal data to be lawful, fair, and proportionate. This article highlights key judicial decisions, including *Folashade Molehin v. UBA and PDPA v. Nizamiye Hospital*, alongside international principles such as GDPR Article 6, to demonstrate that public records containing personal information cannot be disclosed without lawful justification. It concludes by recommending legal, technical, and organizational safeguards such as anonymization, proportionality tests, encryption, and privacy impact assessments to strike a balance between transparency of public documents, and the protection of fundamental privacy rights.

Keywords: Public Documents, Privacy Rights, Data Protection.

INTRODUCTION

The age of digital information has blurred the boundaries between what is public and what should remain private. In Nigeria, this tension recently came into sharp focus when the tax clearance certificate of a well-known political figure surfaced online. Within hours, it was circulating across social media platforms, dissected by citizens, critics, and commentators alike. The document, which ordinarily should confirm compliance with tax obligations, became a lightning rod for questions about wealth, accountability, and trust in institutions.

Yet beneath the spectacle lies a more profound issue. The viral sharing of such a document illustrates how quickly sensitive personal information can escape its intended context once it enters the public domain. A certificate issued by a government authority may carry the label of "public document," but its contents strike at the heart of personal privacy. When such information is disclosed without safeguards, the consequences extend beyond embarrassment or political fallout; they touch on legal rights, institutional credibility, and the very meaning of transparency in a democratic society.

Nigeria's experience is not unique. Around the world, governments wrestle with the paradox of openness: citizens demand transparency to hold leaders accountable, yet individuals also expect their private data to be protected from indiscriminate exposure. In an era where a single upload can make official records go viral, the safeguards around access, purpose, and proportionality become more important than ever.

This incident invites a closer reflection on how society interprets "public records." Should documents be treated as free-for-all simply because they originate from a government office, or must there be boundaries that respect the privacy of individuals? How institutions answer these questions will not only determine compliance with the law but also shape public trust in governance. More importantly, it will reveal whether Nigeria can strike a sustainable balance between the openness required for democracy and the privacy that preserves dignity in the digital age.

WHAT ARE PUBLIC DOCUMENTS?

By virtue of the Evidence Act 2022 (as amended)[1], public documents in Nigeria are broadly defined to include "documents forming the official acts or records:

(i) the sovereign authority
(ii) official bodies and tribunals, or
(iii) public officers, whether legislative, judicial, or executive, in Nigeria or elsewhere; as well as public records of private documents kept in Nigeria.

In practice, this covers virtually any record produced by a government agency in the course of official business, from laws and legislative enactments to court judgments, tax filings, and official certificates, a wide range of documents fall within the category of public records. Court processes such as pleadings, motions, rulings, and final orders are also regarded as public documents once filed, although access is regulated through established court procedures and, in certain sensitive matters such as matrimonial causes, adoption, or cases involving minors, subject to judicial discretion.

Other examples include incorporation documents and annual returns filed with the Corporate Affairs Commission, registered land titles and deeds kept at land registries, voters' registers and election result sheets maintained by the Independent National Electoral Commission, as well as archived government records preserved under the Public Archives Act.

Beyond the Evidence Act, other statutes also treat certain categories of documents as public. The Freedom of Information Act 2011 affirms the right of access to government-held records while carving out exemptions for personal data. The Companies and Allied Matters Act 2020 requires filings like incorporation documents and annual returns with the Corporate Affairs Commission, which then become publicly accessible. Similarly, the Land Use Act and state land registration laws classify registered titles and deeds as public records, while the Electoral Act 2022 makes voters' registers and election result sheets available for inspection. Court rules also reinforce the principle that certain official filings and archived government records fall within the public domain. However, just because a document is "public" for evidentiary or regulatory purposes does not automatically mean its contents can be freely broadcast or repurposed. Public-document status primarily relates to admissibility in court and basic inspection rights.

For instance, Section 104(1) of the Evidence Act states that

> ***"Every public officer having the custody of a public document which any person has a right to inspect shall give that person on demand a copy of it on payment of the legal fees prescribed in that respect, together with a certificate written at the foot of such copy that it is a true copy of such document or part of it as the case may be."***

In short, any person has the right to obtain certified copies of official records but only from the custodian and for legitimate uses. However, a protruding question is whether a public document obtained through the laid down procedures of applicable laws can be used for purposes other than that for which they were obtained?

TO WHAT EXTENT CAN A PUBLIC DOCUMENT BE ACCESSED BY PEOPLE?

Nigeria's constitutional and statutory framework reflects a dual commitment to transparency and privacy. The Constitution of the Federal Republic of Nigeria 1999 (as amended) (CFRN) guarantees both the right to freedom of expression, which underpins access to information, and the right to privacy of citizens, their homes, correspondence, and communications.[2] This sets the foundation upon which subsequent legislation on public records and personal data has been built.

Nigeria's Freedom of Information Act 2011 (FOIA) and the Evidence Act (Amendment) 2023 further empower citizens to request public records, but they draw clear privacy lines. FOIA[3] affirms that anyone can request access to government-held information, and public agencies must proactively publish details of their operations. Yet the FOIA[4] explicitly exempts personal data from disclosure, mandating that a public body "must deny an application for information that contains personal information." Notably, FOIA lists "information required of any taxpayer in connection with the assessment or collection of any tax" as an exempt category.[5] In plain terms, tax records and other confidential files cannot be disclosed without consent. The only exceptions are narrow, permitting disclosure where the data subject consents or the information is already in the public domain, or where the public interest in disclosure clearly outweighs privacy concerns.[6]

The Nigeria Data Protection Act 2023 (NDPA) strengthens this balance by enshrining privacy as a fundamental right and creating the Nigeria Data Protection Commission (NDPC) to oversee compliance. The Act makes it unlawful to process personal data without a valid legal basis such as consent, contractual necessity, legal obligation, vital interests, public interest, or legitimate interest. These lawful bases mirror international standards like the European Union's General Data Protection Regulation (GDPR) Article 6, with strong emphasis on purpose limitation and data minimization. Importantly, the NDPA applies even to records that qualify as public documents. This means personal identifiers within official records remain protected. Leaking a tax clearance certificate without consent or lawful justification would therefore amount to a breach.

Other statutes reinforce these principles. The Companies and Allied Matters Act (CAMA) 2020 requires filings with the Corporate Affairs Commission (CAC) which makes them accessible as public records, but does not remove the obligation to protect personal data within those filings. The Land Use Act and land registration laws[7] deem land titles and deeds as public records, subject to inspection upon payment of fees. The Electoral Act 2022 makes voters' registers and result sheets accessible, while court rules ensure that judgments and pleadings are public documents, albeit with discretion applied in sensitive cases. Each of these laws embodies the balance between legitimate access and the safeguarding of personal privacy.

In short, Nigerian law grants a right of access to official records, but it simultaneously upholds an individual's right to privacy. Transparency and data protection are not mutually exclusive; rather, they are meant to function in tandem, ensuring that openness in governance does not come at the expense of human dignity.

PRIVACY VS. PUBLIC INTEREST IN DISCLOSURE

The law recognizes that in some circumstances, revealing personal information may serve a legitimate societal purpose, while in others, it amounts to an outright violation of privacy. Not all data leaks are unlawful as the context matters.

Fair disclosure refers to sharing personal data when there is a lawful basis and a legitimate purpose. For example, a journalist exposing corruption or a court case might rely on a public-interest justification. But privacy breaches occur when personal data are disclosed without consent or legal ground, causing harm. Such breaches may result from hacking, unauthorized sharing, or human error, leading to identity theft, financial loss, reputational damage, and legal consequences.

The NDPA[8] and the General Application and Implementation Directive (GAID) 2025[9], the lawful bases for processing personal data include consent, contractual and legal obligations, vital interests, public interest, and legitimate interest. These principles align closely with Article 6 of the European Union's General Data Protection Regulation (GDPR), which similarly underscores the importance of transparency, purpose limitation, and fairness in the lawful processing of personal data.

While access to information is important for openness and accountability in a democratic society. However, releasing information in the name of public interest must always be proportionate, necessary, and carefully limited. Even where disclosure is justified, the data should only be used for the specific purpose for which it was obtained, while protecting the individual's privacy. Sensitive details such as financial records, health information, or biometric data usually require explicit consent, and sharing them without it is almost always unlawful.

The case of *PDPA v. Nizamiye Hospital*[10] illustrates the delicate balance between individual privacy rights and wider societal concerns. Although the hospital relied on arguments of safety and voluntary data use, the court found no clear breach. The court underlined that fairness and transparency must remain central to any disclosure of personal information.

Essentially, public interest, however important, should never be treated as a blanket justification for eroding privacy rights. Consent remains the highest standard, and all data processing must be guided by the principle of minimization. Where organizations fall short, the sanctions provided under the NDPA 2023 including fines and possible imprisonment act as essential safeguards to secure accountability.

BEST PRACTICES AND SAFEGUARDS

Organizations, governments, and institutions worldwide face the challenge of balancing transparency with individual privacy in a digital age. Nigeria's Data Protection Act 2023 strengthens this balance through clear legal frameworks. However, achieving it requires legal, organizational, and technical safeguards working in harmony.

A. Legal Safeguards

1. Data Minimization: Institutions should disclose only the minimum personal information necessary for transparency objectives.

2. Anonymization and Pseudonymization: Sensitive data should be anonymized before publication, ensuring that individuals cannot be directly identified.

3. Balancing Test: Before disclosure, authorities should apply a proportionality assessment: access public interest against privacy harm. This mirrors the GDPR's "legitimate interest" test.

4. Clear Legal Basis: Data should only be disclosed when there is a lawful justification, such as a statutory requirement, consent, or overriding public interest. The Federal High Court in *United Bank of Africa (UBA) v Folashade Molehin*[11] recognized the unalterable right to consent and purpose limitation by data processors and controllers when dealing with sensitive data of data subjects.

B. Institutional Safeguards

1. Data Protection Officers (DPOs): Under the NDPA, organizations handling large volumes of data must appoint DPOs, who can guide decisions on whether and how to disclose personal data.

2. Privacy Impact Assessments (PIAs): Before major disclosures, institutions should conduct PIAs to identify risks and mitigation measures. DPIAs help in identifying and mitigating potential privacy risks associated with new projects or systems before they are deployed.[12]

3. Tiered Access: Instead of full public disclosure, access can be stratified: regulators may access full datasets, while the public receives aggregated or redacted information.

C. Technical Safeguards

1. Encryption and Secure Platforms: Encryption protects shared data from unauthorized access by converting it into unreadable formats. Strict access controls and security measures further safeguard sensitive information. End-to-end encryption in messaging apps ensures only the sender and recipient can view the content.[13]

2. Adopting privacy-enhancing technologies such as anonymization and pseudonymization to help in reducing the risks associated with personal data processing by making it more difficult to identify individuals from the data[14].

3. Audit Trails: Maintaining records of who accessed or disclosed data helps ensure accountability and reduces the risk of misuse.

RECOMMENDATIONS AND FUTURE INSIGHTS

To strengthen privacy in Nigeria's public records era, stakeholders should:

- **Monitor NDPC Guidance:** Stay updated on regulations and consult with the Nigeria Data Protection Commission. As the NDPA and GAID evolve, guidance notices and industry consultations will clarify expectations.

- **Implement Clear Policies:** Develop strict internal protocols for data access. Enforce "need-to-know" sharing and use emerging tech like blockchain to transparently track data provenance and access rights.[15]

- **Leverage Privacy-Preserving Tech:** Adopt blockchain and decentralization for record-keeping where feasible. For instance, citizen-owned digital IDs or personal data vaults can give individuals control over who sees their data. Use Privacy-Enhancing Technologies (PETs) to enable data use without exposing raw personal data.

- **Invest in Awareness and Tools:** Educate the public about privacy rights and equip them with tools (like consent dashboards) to manage their data. Clear notices on how personal data will be used can foster trust. Citizen literacy campaigns can help people understand why their tax or medical information is protected.

- **Engage Multi-Stakeholder Efforts:** Government, industry, and civil society should collaborate on best practices. Join or form cross-sector privacy forums and standards bodies. Working together (for example on model consent frameworks or redaction standards) ensures a consistent approach.

These steps will help Nigeria keep pace with its digital transformation. By combining legal rigor with smart technology and public engagement, we can make transparency and privacy mutually reinforcing goals.

CONCLUSION

In the digital age, unchecked exposure of personal data undermines trust and dignity. The viral leak of a politician's tax certificate should be a wake-up call: simply labeling something a "public document" does not erase privacy rights. Nigeria's new Data Protection Act is a strong shield, but real protection demands more. It requires principled practice by public bodies, sophisticated privacy tech, vigilant enforcement, and an informed citizenry. As one court warned, public interest cannot be a blanket excuse to trample privacy. If Nigeria fails to act now, we risk normalizing surveillance and corroding individual rights. Protecting personal data is more than a legal box-check; it's about preserving human dignity. In the end, an open society must also be a respectful one - ensuring transparency with privacy, not at its expense.

REFERENCES

[1] Section 102, Evidence Act 2022 (as amended)
[2] Section 37, Constitution of the Federal Republic of Nigeria 1999 (as amended)
[3] Sections 1 and 2 Freedom of Information Act 2011
[4]Section 14(1) Ibid.
[5] Section 12 and 15, Ibid.
[6] Sections 14(10 & (2) Ibid.
[7] Section 3, Lagos State Land Registration Law 2015
[8] Section 25, Nigerian Data Protection Act 2023
[9] Article 16, General Application and Implementation Directives 2025.
[10] FCT/HC/GAR/CV/187/2024
[11] PIN Strategic Litigation: United Bank of Africa (UBA) ordered to pay customer N8,000,000 for gross violation of her right to data privacy, (Paradigmhq June, 2024), <https://paradigmhq.org/press-release-united-bank-of-africa-uba-ordered-to-pay-customer-n8000000-for-gross-violation-of-her-right-to-data-privacy/> accessed 2nd September 2025
[12] Cavoukian, A. (2011). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada
[13] Sweeney, L. (2017). Privacy and confidentiality. Cambridge University Press.
[14] Tadayoni, R., & Yadati, N. (2020). Privacy-enhancing technologies: A review. Journal of Information Privacy and Security, 16(1), 29-46.
[15] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (180-184).

DISCLAIMER:

The information provided in this publication does not, and is not intended to constitute legal advice. It is intended for general informational purposes only. Please contact us for further information.

Email: info@syntegrallp.com
© Copyright 2025 - Syntegral Legal Practice