

THE LEGAL AND INSTITUTIONAL FRAMEWORKS GOVERNING TAXPAYER DATA PROTECTION IN NIGERIA AND SOUTH AFRICA.

By

Zhihwi Dauda Esq. (LL. B, B.L, LL.M, ACE, FCIT, PGDE)

E-mail: thihwi.dauda@nrs.gov.ng / daudathihwi@gmail.com Phone: +2348059538671

Central Business District, Abuja -FCT, West Africa.

ABSTRACT

The digitalization of tax administration has made taxpayer data one of the most sensitive assets held by the state. This article examined the legal and institutional frameworks governing taxpayer data protection in Nigeria and South Africa, using a doctrinal and comparative approach. In Nigeria, the framework rests on Section 37 of the Constitution of the Federal Republic of Nigeria, 1999, Data Protection Act 2023, the Nigeria Data Protection Regulation (NDPR) 2019, the Nigeria Revenue Service (Establishment) Act (NRSEA), 2025, the Nigeria Tax Administration Act (NTAA), 2025, and the Freedom of Information Act (FOIA) 2011. The Nigeria revenue service (NRS) has now expanded powers to collect, store, and share personal and financial data for tax administration, fraud prevention, and Common Reporting Standard exchanges, but this is tempered by confidentiality duties, security obligations under Section 38 NDPA, and oversight by the Nigeria Data Protection Commission (NDPC). Nigerian courts have interpreted the constitutional right to privacy narrowly, the FOIA exempts taxpayer data, though public concern over MoUs like the NRS-France arrangement highlights transparency deficits. South Africa's regime is anchored in Section 14 of the Constitution of the Republic of South Africa, 1996, Protection of Personal Information Act No. 4 (POPIA), 2013, the Tax Administration Act No. 28 (TAA), 2011, the SARS Act 1997, and Promotion of Access to Information Act No. 2 (PAIA), 2000. The POPIA, 2013 imposes eight lawful-processing conditions and is enforced by the Information Regulator, while the TAA 2011 creates a strict secrecy regime with codified exceptions. The Constitutional Court in *Arena Holdings v SARS* (2023) limited absolute secrecy by reading a public interest override into PAIA 2000. Both countries recognize taxpayer confidentiality, criminalize unauthorized disclosure, and participate in Common Reporting Standard and Article 26 exchanges. However, they face shared challenges: cybersecurity failures, expanded data collection powers without tax-specific proportionality limits, weak institutional enforcement, low digital literacy and trust, misalignment between tax treaty data flows and data protection law, and the rise of AI driven profiling without adequate safeguards. The paper argued that while Nigeria has a strong normative foundation and South Africa has a more mature enforcement model, both must strengthen oversight, transparency, and taxpayer engagement to sustain voluntary compliance in a data driven tax system.

Key words: **Institutional Frameworks, Taxpayer, Data Protection, Nigeria, South Africa**

1.0 Introduction:

The future of tax administration lies in the intelligence generated from taxpayer's financial data, hence it is data intensive¹. Revenue authorities collect identity details, income or financial records, bank transactions, property ownership, and cross-border financial data obtained through automatic exchange of information². Exchange of information is an essential tool for tax authorities worldwide to ensure that all taxpayers pay the correct amount of tax. Whilst cross-border movement of goods, services and persons were intensifying, tax authorities were facing obstacles in obtaining information about the international transactions, offshore assets and financial affairs of their residents. This scenario has changed: tax administrators have worked together and engaged in worldwide co-operation through exchange of information in tax matters.³ Digitalisation through e-filing, e-invoicing, and real-time reporting has improved compliance and revenue yield in Nigeria⁴. Recently, South Africa is keying into digitalization

of its VAT administration as it positioned e-invoicing and VAT digital reporting as central components of its long-term strategy to modernize tax administration, enhance compliance, and improve revenue collection efficiency.⁵

The concentration of sensitive data creates acute privacy risks⁶. A breach or misuse erodes public trust, reduces voluntary compliance, and exposes states to legal liability. The tension is clear: revenue authorities require broad powers to ensure tax compliance, while taxpayers have a legitimate expectation that their data will be used only for lawful tax purposes and kept confidential. Nigeria and South Africa are instructive comparators. Both have enacted comprehensive data protection legislation and recognise taxpayer confidentiality in tax statutes, yet their regulatory trajectories differ.

2.0 CONCEPTUAL AND THEORETICAL FRAMEWORK

a) Taxpayer Data and the Right to Privacy:

Taxpayer data is any personal, financial, and identifying information that individuals and businesses provide to tax authorities.⁷ It is also regarded as any identifiable information collected, processed, or held by a government tax authority regarding an individual's or business's tax liability, financial standing, and personal identity.⁸ On the other hand, privacy in the tax context is a qualified right to control personal information and prevent its use beyond the purpose for which it was collected.⁹ Internationally, this is grounded in Article 12 of the Universal Declaration of Human Rights (UDHR) 1948¹⁰ : *“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”* This provision is mutatis mutandis with the provision of Article 17 of the International Covenant on Civil and Political Rights 1966¹¹. It is worth noting that the above Article 12 of the UDHR, 1948 directly establishes privacy as a fundamental human right by prohibiting any arbitrary interference by the State or third parties with an individual's privacy, family life, home, and correspondence, and by further protecting a person's honour and reputation from attack.

It is the opinion of the writer that the term “arbitrary” used in the above provision is deliberate and central, it means that any interference will not only be unlawful, but will also unjust, unreasonable, or disproportionate, thereby requiring that limitations on privacy be prescribed by law, pursue a legitimate aim, and be necessary in a democratic society. By expressly listing the family, home, and correspondence alongside privacy, the provision recognises both physical and communicational spheres of self-rule as deserving protection from surveillance, search, seizure, interception, and disclosure by agencies of State including relevant Tax Authority. The second phrase imposes a positive duty on States to provide “the protection of the law,” meaning that legal systems must create effective remedies, oversight mechanisms, and accountability structures to prevent, investigate, and redress violations, whether committed by public authorities or private actors. In the tax context, this provision is particularly relevant because the collection and centralisation of taxpayer data by revenue authorities in Nigeria (NRS) and in South Africa (SARS) constitute an interference with privacy and correspondence, and is therefore only permissible where it is authorised by law, serves the legitimate purpose of revenue collection, and is balanced by safeguards such as purpose limitation, confidentiality, data security, and independent oversight.

Both Nigeria and South Africa are Member States of the African Union. While the African Charter on Human and Peoples' Rights (ACHPR), 1981¹² does not contain an express and stand-alone provision on the right to privacy, aspects of this right may be inferred from several of its provisions, including Article 4 on the right to life and personal integrity, Article 5 on respect for human dignity, and Article 6 on liberty and security of the person. To further strengthen the protection of personal data across the continent, the African Union adopted the

Convention on Cyber Security and Personal Data Protection, commonly known as the Malabo Convention, on 27th June, 2014 in Malabo, Equatorial Guinea, as the first continent-wide legal framework to address cybersecurity and data protection¹³. It was conceived to harmonize Africa's response to rising cybercrime, promote digital trust, and protect personal data amid rapid digitalization, with the goal of creating a safe cyberspace for economic development and integration. The Convention sets out four core pillars: cybersecurity, protection of personal data, electronic transactions, and the promotion of e-governance. However, it took nearly 9 years to attain the required 15 ratifications and it finally came into force on 8th June, 2023, making it legally binding on ratifying States.

The African Union Convention on Cybersecurity and Personal Data Protection ,2014¹⁴ Article 8 Chapter II (Personal data protection) provides:

“Objective of this Convention with respect to personal data

1. Each State Party shall commit itself to establishing a legal framework aimed at strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punish any violation of privacy without prejudice to the principle of free flow of personal data.

2.The mechanism so established shall ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognizing the prerogatives of the State, the rights of local communities and the purposes for which the businesses were established”

Since the ratification of the Convention by member State, it has served as the benchmark for national data protection laws in Africa, including Nigeria Data Protection Act (NDPA) 2023 and South Africa's Protection of Personal Information Act (POPIA) 2013, by obligating States to enact legislation on data subject rights, lawful processing, cross-border data transfers, and to establish independent data protection authorities

b) Reconciling Nation's Tax Authority Compliance Powers with Individual Data Protection Rights

The IMF (2021) working paper¹⁵ contends that the digital transformation of tax administration has made expansive access to financial data sets a functional necessity for modern revenue authorities seeking to enhance compliance and protect public revenue. By leveraging Risk-focused digital auditing, data analytics, and cross-border information exchange, authorities such as NRS and SARS are able to detect anomalies, identify under reporting, and disrupt illicit financial flows that transcend jurisdictional boundaries. However, this aggressive accumulation and processing of taxpayer data generates a fundamental legal tension: on one hand, the State has a legitimate interest in efficient domestic revenue mobilization to fund public goods and meet fiscal obligations; on the other hand, taxpayers retain constitutionally guaranteed rights to financial privacy and data security, as protected under Section 37 of the Constitution of Federal Republic of Nigeria 1999 as (Amended) and Section 14 of the Constitution of the Republic of South Africa, 1996 and as operationalized through the NDPA, 2023 and POPIA, 2013 respectively. Consequently, the imperative to maximize tax collection must be reconciled with principles of legality, proportionality, purpose limitation, and accountability, such that data collection is not excessive, is adequately safeguarded against misuse, and is subject to independent oversight and effective remedies to prevent the erosion of trust that underpins voluntary tax compliance.

Data protection advocates argue that granting tax authorities unchecked powers to collect, share, and process taxpayer information creates chilling effects, enables abuse, and exposes

sensitive data to significant risk. Without clear purpose limitation and data minimisation, such powers can lead to bulk collection and secondary use of information beyond what is necessary for tax assessment. The lack of strong access controls, independent oversight, and effective remedies further increases the risk of misuse, leaks, and violations of privacy, undermining trust and discouraging voluntary compliance.¹⁶

In South African for instance, **Amanda Vissera** in her article ‘Deep Flaws In SARS’s Systems, Office of the Tax Ombud Investigation Finds’¹⁷ reported that the South Africa’s Office of the Tax Ombud’s draft report on e-Filing profile hijackings reveals deep systemic failures within SARS that have violated fundamental taxpayer rights to timely service, information, fair treatment, and protection from harm, with fraudsters exploiting weaknesses in authentication and security to gain unauthorised access, alter banking details, and redirect refunds while SARS’s slow detection and resolution mechanisms left victims waiting months or years for relief and even subjected them to debt collection before fraud was cleared. The author stated further that, South African Tax Practitioners United (SATPU) criticised the report for inadequately addressing the bypassing of two factor authentication (2FA), unauthorised banking changes, and practitioner lockouts, and warned that the pattern suggests possible internal collusion, which is why it supports the Office of the Tax Ombud’s recommendation for an independent Inspector General with powers to investigate high risk areas and publish transparent reports. The author however reported that:¹⁸ In response, South Africa Revenue Service has acknowledged the findings and committed to enhancing authentication protocols, including compulsory and graded 2FA, improving fraud-risk detection, optimising refund-verification systems, issuing alerts for high-risk profile changes and after-hours refunds, and strengthening collaboration with banks, Companies and Intellectual Property Commission (CIPC), and the SAPS, while the Ombud and SATPU stress that because cybercrime is evolving and involves interconnected institutions, urgent implementation of these measures is essential not only to stop e-filing hijacking but also to restore taxpayer trust and uphold the integrity of South Africa’s tax administration system.

Nigerian legal experts have also engaged with this issue. A recent law firm briefing titled Analysis of Income-Tracking & Constitutional Risk examined how large-scale digital asset tracking, international data exchange, and data privacy concerns intersect under the Constitution. Banwo & Ighodalo¹⁹ the author argued that while the Nigeria Tax Act (NTA) 2025 and Nigeria Tax Administration Act (NTAA), 2025 grants the Nigeria Revenue Service broad powers to track income through mechanisms like Common Reporting Standard data exchange, mandatory bank reporting under section 29 of the NTAA 2025, and targeting of digital assets and remote workers, these powers raise significant data abuse concerns if not properly constrained. The authors noted the public fears specifically around the undisclosed MoU with France’s Direction Générale des Finances Publiques (DGFIP) regarding potential mass surveillance, loss of economic control, and geopolitical manipulation, though the NRS has stated it involves only technical assistance.²⁰ Legally, section 25(1)(b)(ii) of the NDPA 2023 permits such data processing as a statutory obligation, but prohibit “voyages of discovery” and require compliance with principles of necessity, proportionality, purpose limitation, and transparency. Hence, such processing remains subject to strict confidentiality obligations under the NRS as mandated under section 142 of the NTAA. The core concern expressed is not income tracking itself, but implementation abuse: indiscriminate bulk collection of financial data beyond what is tax relevant, lack of transparency on what data is collected and why, and secondary use of taxpayer data without clear authorization. The necessity for both countries to strike a balance in taxpayer’s data protection through purpose limitation, data minimisation, access controls, independent oversight, and provision of effective remedies is desirable.

c) International Standards:

National practice on taxpayer data access and exchange is shaped by two core international regimes: Organisation for Economic Co-operation and Development (OECD)/ Common Reporting Standard for Automatic Exchange of Information (AEOI), and Article 26 of the OECD Model Tax Convention.²¹ These frameworks expand tax authorities' ability to obtain and share taxpayer information across borders, taxpayer data protection is embedded as a legal prerequisite rather than an afterthought. Both regimes impose strict confidentiality obligations, limiting the use of exchanged information for tax purposes only and restricting disclosure to persons directly involved in tax administration, assessment, or enforcement. Participation in CRS/AEOI is further conditioned on the Global Forum peer review of a jurisdiction's data security, IT systems, and safeguards, with suspension from receipt of information as a sanction for non-compliance. Nevertheless, the large-scale cross border transfer of personal and financial data inherently carries risks of abuse, breach, or unauthorised disclosure by officials. To address this, domestic laws in most jurisdictions criminalise unlawful disclosure and provide taxpayers with rights of access and correction, seeking to balance the goal of tax transparency with the need to protect taxpayer privacy and prevent exposure of sensitive data to the wrong hands. The research briefly examined the two core international regimes.

The Common Reporting Standard is the OECD's global standard for the automatic exchange of financial account information between tax authorities. Under Common Reporting Standard, financial institutions in participating jurisdictions identify tax residents of other countries and report details on accounts including name, address, TIN, account balance, and income to their domestic tax authority. This information is then automatically exchanged with the tax authority of the account holder's country of residence on an annual basis, without the need for a specific request. The goal is to detect offshore tax evasion and improve voluntary compliance by closing information gaps. Participation requires meeting Global Forum standards on confidentiality, data safeguards, and proper use of information. As of 2026, over 100 jurisdictions exchange data under CRS and the OECD Common Reporting Standard.²²

Article 26 of the OECD Model Tax Convention was recently amended, expanding the scope and flexibility of tax information exchange. The updates expressly permit a receiving jurisdiction to use information obtained through exchange not only for the tax matters of the person originally concerned, but also for tax matters relating to other persons, and to do so without first seeking authorisation or giving notice to the sending jurisdiction. The revisions further provide agreed guidance on taxpayer access to exchanged information and on the treatment of "reflective non-taxpayer specific information," stipulating that standard confidentiality rules continue to apply, and that such information may only be disclosed to third parties if it is anonymised and both states agree in writing that disclosure will not impair tax administration. By clarifying permitted uses and reaffirming confidentiality obligations, the amendments give tax authorities greater flexibility to manage and share information, while also signalling to multinational enterprises the importance of maintaining consistent documentation and coordinated approaches across jurisdictions.²³

Nigeria and South Africa are both members of the Global Forum on Transparency and Exchange of Information for Tax Purposes. The Global Forum conducts peer reviews to assess members' implementation of international standards for information exchange, including the Common Reporting Standard/Automatic Exchange of Information (CRS/AEOI) and Exchange of Information on Request (EOIR) under Article 26 and similar provisions. Membership of the

Global Forum commits countries to a legal framework that allows access to bank and ownership information, confidentiality and data protection safeguards for exchanged information, Practical implementation, including competent authority agreements and IT systems for secure transmission. Through the Global Forum, both countries are therefore required to align domestic tax secrecy, data protection, and procedural rules with these international standards, while also undergoing periodic review of their compliance and effectiveness. Therefore, Common Reporting Standard drives automatic bulk data exchange, Article 26 enables targeted information requests, and Global Forum membership binds both countries to implement these standards with confidentiality and taxpayer rights safeguards.

3.0 THE NIGERIAN FRAMEWORK FOR TAXPAYER DATA PROTECTION

The protection of taxpayer personal data in Nigeria is governed by a combination of constitutional provisions, data protection legislation, tax statutes, and access to information laws. This section outlines the key legal and institutional framework that regulates the collection, use, and disclosure of taxpayer information in Nigeria. I shall now discuss these legal instruments as follows:

a) Constitutional Foundations

In Nigeria, since the 1960²⁴ Independence Constitution, through 1979²⁵ and 1999, The Constitution has always treated privacy as a fundamental right. Section 37 of CFRN, 1999 (as Amended)²⁶ provides: *"The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected"* The right to privacy covers a wide range of issues such as confidential correspondence, email and internet use, medical history, personal data, eavesdropping, sexual orientation and personal life styles.

According to Solove,²⁷ the right of privacy is considered as any activities that are intended to be excluded from the knowledge of others. Solove further argued that: *"The value of privacy must be determined on the basis of its importance to society, not in terms of individual rights. Moreover, privacy does not have a universal value that is the same across all contexts. The value of privacy in a particular context depends upon the social importance of the activities that it facilitates."*²⁸ The right of privacy implies the exclusion of the public eye from prying into an individual's affair. Another crucial aspect of the right to privacy entails the right to protect one's image and personality and to have unfettered access to control one's zones of exclusivity, space and confidential information. The right to privacy lies within the realm of self-ownership. It is the moral liberty of doing what an individual deems fit to be done with his/her individualism and keeping others outside the sphere of his/her self-ownership²⁹

The right to privacy of citizens as guarantee under the Nigerian constitution received judicial interpretation in the case of **NWALI v EBSIEC & ORS (2014) LPELR-23682(CA) Per AGIM, J.C.A (Pp. 27-29 paras. E-E) where the court held:**

"S. 37 of the 1999 Constitution states that "the privacy of citizens, their homes, correspondence, conversations and telegraphic communication telephone guaranteed and protected". It is clear from the text of the provision that it specifically mentioned the types of privacy that it protects. Five of them are listed therein as follows- 1. The privacy of citizens 2. The privacy of their homes 3. The privacy of their correspondence 4. The privacy of their telephone conversations 5. The privacy of their telegraphic communication. These are clearly restated by this Court in Federal Republic of Nigeria v Daniel (2011) 4 ELR 4152 thus- "Undoubtedly, by virtue of the Provision of Section 37 of the 1999 Constitution, the privacy of every Nigerian citizen, the home, correspondence, telephonic and telegraphic communications are cherishingly guaranteed and protected.

The trial Court in stating the scope of the said right, listed the aspects of privacy S.37 contemplates as follows-

- 1. Privacy at home*
- 2. Privacy of one's communication*
- 3. Privacy in private family and matters incidental thereto.*

I understand privacy of one's communication as used by the trial Court to mean privacy of correspondence, privacy of telephone conversations and privacy of telegraphic communication. It excluded the privacy of the citizens expressly provided for in S. 37 of the Constitution and included privacy of private family life and matters incidental thereto not expressly provided for in the text of the provision. The privacy of home, privacy of correspondence, privacy of telephone conversations and privacy of telegraphic communication are clear and particular as to the nature of privacy protected or the area or activity in respect of which a person is entitled to enjoy privacy. It is obvious that the right to the privacy of the person's decision and choice of candidate to vote for cannot be enjoyed as part of the privacy of his home, the privacy of his correspondence, the privacy of his telephone conversation and the privacy of his telegraphic communication. It is glaring that the phrase "Privacy of Citizens" is general and is not limited to any aspect of the person or life of a citizen. It is not expressly defined by the Constitution and there is nothing in the Constitution or any other statute from which it's exact meaning or scope can be gleaned."

The decision of Nigerian Court of Appeal above shows that section 37 of the 1999 Constitution expressly guarantees five categories of privacy: the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications. The Court observed that while the phrase "privacy of citizens" is general and undefined, the specific categories listed do not extend to a citizen's right to privacy in the choice of candidate to vote for. The decision thus reflects a narrow, textual interpretation of section 37, limiting its scope to the particular areas expressly mentioned and highlighting that the general aspect of "privacy of citizens" lacks a defined constitutional or statutory meaning. What then is the scope of the right to privacy of a citizens? The Nigeria Court of Appeal in the latter case of **In Incorporated Trustees of Digital Rights Lawyers Initiative & ORS v NIMC (2021) LPELR-55623(CA) PER MOHAMMED, J.C.A at (PP. 25-27 PARAS. E)**, stated

In highlighting the absence of a clear scope of the right to "privacy of citizens" as guaranteed under Section 37 of CFRN, 1999, this Court, per Agim, JCA (as he then was, now JSC), had held in the cited case of NWALI v. EBSIEC (2014) LPELR-23682(CA) at pages 27 - 29, para. E, as follows: The meaning of the term "privacy of citizens" is not directly obvious on its face. It is obviously very wide as it does not define the specific aspects of the privacy of citizens it protects. A citizen is ordinarily a human being constitution of his body, his life, his person, thought, conscience, belief, decisions (including his plans and choices), desires, his health, his relationships, character, possessions, family, etc. So how should the term "privacy of citizens" be understood? Should it be understood to exclude the privacy of some parts of his life? This can be seen from its holding that the right includes "privacy in private family life and incidental matters when this aspect is not expressly provided for in that Section and that meaning is not patently obvious from the text of that Section...The privacy of home, privacy of correspondence, privacy of telephone conversations and privacy of

telegraphic communication are clear and particular as to the nature of privacy protected or the area or activity in respect of which a person is entitled to enjoy privacy... It is glaring that the phrase "Privacy of Citizens" is general and is not limited to any aspect of the person or life of a citizen. It is not expressly defined by the Constitution and there is nothing in the Constitution or any other statute from which its exact meaning or scope can be gleaned. (underline mine for emphasis) As observed above by His Lordship Agim, JCA (as he then was), the privacy of the home, correspondence, telephone and telegraphic communications protected by the Section are clearly definable and determinable as to their nature and scope. But the meaning and scope of "privacy of citizens" as guaranteed by the Section has not received clear definition/interpretation in the Constitution. The trial Court had, in my view, rightly held above, that the right to "privacy of citizens" as guaranteed under the Section includes the right to protection of personal information and personal data.

The decision of the Nigerian Court of Appeal in the above case demonstrates that the scope of the right to privacy under section 37 of the 1999 Constitution is not exhaustively defined by the text of the Constitution itself. The provision guarantees privacy of *"citizens, their homes, correspondence, telephone conversations and telegraphic communications,"* but it does not expressly mention modern concerns such as personal data and digital information. This textual silence has left the right open to judicial interpretation. In the opinion of the writer, this ambiguity confers a legitimate interpretive role on the courts to expand or widen the scope of the right in line with changing social, technological, and legal realities. By holding that data protection is implicit in section 37, the Court of Appeal adopted a purposive and evolutionary approach, recognizing that constitutional rights must not be confined to the understanding of 1999, but must be given meaning that protects citizens in the contemporary digital age. Thus, the judgment illustrates that the undefined nature of the right under the Constitution is not a weakness, but rather an avenue for judicial development to ensure the right to privacy remains relevant and effective.

The pertinent question raised by the writer is whether the constitutional right to privacy extends to the protection of taxpayer data? The right to privacy guaranteed under section 37 of the Constitution of Federal Republic of Nigeria 1999 (As amended) is not absolute. Like other fundamental rights in Chapter IV, it is subject to lawful derogations where the interest of the State or the public outweighs individual interests. Section 45(1) of the Constitution of Federal Republic of Nigeria 1999 (As amended) permits limitation of the right to privacy where such limitation is reasonably justifiable in a democratic society in the interest of defence, public safety, public order, public morality, public health, or for the purpose of protecting the rights and freedoms of other persons. Consequently, while the Constitution guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications, it does not shield these interests from legitimate State actions such as tax administration, criminal investigation, national security operations, and lawful data collection. Thus, the right operates within a framework that balances individual autonomy with competing public interests. For the avoidance of doubt section 45(1) of the Constitution of Federal Republic of Nigeria 1999 (As amended) provides ***"Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society – (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom of other persons"***

To answer the question as to whether the constitutional right to privacy extends to the protection of taxpayer data. The writer is of the opinion that the constitutional right to privacy under section 37 of the Constitution of Federal Republic of Nigeria 1999 (As amended) does not expressly extend to taxpayer data. In **Nwali v EBSIEC** supra, the Nigerian Court of Appeal adopted a narrow, textual reading and held that section 37 protects only the privacy of citizens, homes, correspondence, telephone and telegraphic communications, and does not cover a general "privacy of citizens" right. Taxpayer information held by government agencies is therefore generally regarded as subject to disclosure for public-interest purposes such as tax administration, especially given that section 45(1) permits limitation of the right to privacy where reasonably justifiable in a democratic society for public revenue and order.

b) Nigeria Data Protection Act 2023:

The NDPA 2023 applies to data controllers and processors of personal data domiciled, resident, or operating in Nigeria.³⁰ The Nigerian tax authority is statutorily empowered to access taxpayers' personal data for tax administration purposes. Section 25 of the NDPA considers data processing as lawful where the data subject has given consent, or where it is necessary for contract performance, legal compliance, protection of vital interests, performance of a public task, or for legitimate interests of the controller/processor/third party. However, processing based on legitimate interests is not lawful if it overrides the data subject's fundamental rights, is incompatible with other lawful bases, or where the data subject would not reasonably expect such processing. For avoidance of doubt Section 25 of the NDPA³¹ provides thus:

(1) Without prejudice to the principles set out in this Act, data processing shall be lawful, where (2) (a) the data subject has given and not withdrawn consent for the specific purpose or purposes for which personal data is to be processed; or (b) the processing is necessary- (i) (ii) for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract, for compliance with a legal obligation to which the data controller or data processor is subject, (iii) to protect the vital interest of the data subject or another person, (iv) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor, or (v) for the purposes of the legitimate interests pursued by the data controller or data processor, or by a third party to whom the data is disclosed. Interests in personal data processing shall not be legitimate for the purposes of subsection (1) (b)(v), where- (a) they override the fundamental rights, freedoms and the interests of the data subject; (b) they are incompatible with other lawful basis of processing under subsection subsection (1)(b) (i)-(iv); or (c) the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.

The power of the Nigerian tax authority to access personal data of taxpayers is not absolute. Section 24 of NDPA sets out data protection principles including purpose limitation and security,³² whenever there is a breach, it must be reported to the NDPC within 72 hours for enforcement.³³ Tax Authorities in Nigeria are bound by international treaties or conventions to which they are signatories for sharing of taxpayers data, however, the NDPA has taken a step further to impose a duty on these Tax Authority to ensure adequate protection in all cross-border transfers.³⁴ Despite the fact that the NDPA provides that, data subject rights can be restricted where necessary for tax assessment and collection, under Section 38 of NDPA³⁵ it made provision for the Security and protection of taxpayers' data, stating that the extent that,

every data controller and processor (Nigeria Revenue Service inclusive) must put in place appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data, protecting it against loss, misuse, alteration, unauthorised access or disclosure. The measures must consider the sensitivity and volume of data, potential harm to data subjects, scope and duration of processing, and the cost and availability of safeguards relative to the size of the organisation. Acceptable measures include pseudonymisation, encryption, secure and resilient processing systems, data recovery processes, periodic risk assessments, regular testing of safeguards, and continuous updating of security measures to address new risks.

It is important to note that the Nigeria Data Protection Commission (NDPC), established under Section 4 of the NDPA 2023, is not a toothless body. In the enforcement of general data protection, including the protection of taxpayer data, the Commission is vested with statutory powers to investigate violations and impose penalties on offenders. Section 6(g) of the NDPA 2023 empowers the NDPC to impose penalties for any breach of the Act or its subsidiary legislation, giving it real enforcement authority beyond mere advisory functions. This means the Commission can fine, sanction, or take corrective action against data controllers and processors that violate provisions such as unlawful processing, failure to secure data, or non-compliance with data subject rights. The penalties are tiered based on whether the organization is of “major importance,” and serve to deter violations, enforce accountability, and ensure compliance with data protection standards in Nigeria.

The Nigeria Data Protection Act, 2023 is therefore regarded as Nigeria’s key law for protecting personal data privacy, including taxpayer data. It sets clear rules for data handling and gives the NDPC powers to enforce compliance, thereby promoting accountability and aligning Nigeria with global data protection standards.

c) Nigeria Data Protection Regulation (NDPR) 2019

The National Information Technology Development Agency (NITDA) in exercise of its power under section 6 (a) and (c) of its establishment Act,³⁶ on 25th January 2019, issued the Nigeria Data Protection Regulation as a subsidiary legislation. The objectives of the Regulation are to protect individuals’ right to data privacy, ensure safe and trustworthy data transactions, prevent the manipulation of personal data, and enable Nigerian businesses to remain competitive globally by providing a fair, equitable, and internationally aligned data protection framework.³⁷ Interestingly, the scope of the Regulation applies to the processing of personal data of natural persons in Nigeria, regardless of the method or medium used, and also covers Nigerian citizens residing abroad. It governs all transactions involving personal data processing while ensuring that it does not override or diminish any additional privacy rights granted to any person under existing Nigerian law or foreign law, contract, or policy.³⁸

The Nigeria Data Protection Regulation (NDPR) made provision for cross-border Transfers of personal data, it provide to the extent that, Personal data may only be transferred abroad where adequate protection exists or under exceptions like explicit consent, contract necessity, or public interest, subject to oversight by NITDA and the Attorney General.³⁹ As part of implementation & enforcement strategies, the Regulation imposes a mandatory duty on all organizations including Nigeria Revenue Service who uses citizen personal data to as a mandatorily publish its data protection policies, appoint Data Protection Officers, conduct audits, and build capacity.⁴⁰ It went further to provide for the establishment of NITDA Data Protection Compliance Organization (DPCOs) to monitor compliance.⁴¹

The Regulation does not leave an aggrieved citizen whose personal data has been violated without recourse. In addition to the right to seek redress in court, paragraph 4.2(1) establishes an Administrative Redress Panel to handle citizens' complaints within 28 working days. To align with global standards, the Regulation also encourages local and international cooperation.⁴²

d) Nigeria Revenue Service (Establishment) Act 2025:

The Nigeria Revenue Service Establishment Act, (NRSEA) 2025 significantly consolidates and expands the tax authority's powers to collect personal data. Under Section 4(1) (l), (m) and (q),⁴³ the Service has broad powers to collect, store and maintain personal and business data of all taxpayers, including individuals and corporate bodies. It is mandated to keep up-to-date databases, records and statistics for tax administration, fraud prevention, and compliance monitoring, and to issue taxpayer identification numbers to all relevant taxable persons. the section is reproduced below: **Section 4(1)(i)(m) &(q)**

The Service shall:

(l) "provide and maintain access to up-to-date and adequate data and information on all taxable persons, individuals, corporate bodies... for the purpose of efficient, effective and correct tax administration and to prevent tax evasion or fraud"

(m) "maintain database, statistics, records and reports on persons, organisations, proceeds, properties, documents... relating to tax administration including matters relating to tax waivers, fraud or evasion"

(q) "issue taxpayer identification or any other equivalent identity to every relevant taxable person"

As Luke 12:48 (KJV) reminds us, "For unto whomsoever much is given, of him shall be much required." In the same vein, the NRSEA, 2025 grants the Nigeria Revenue Service expanded powers to collect taxpayers' data for tax administration. With this expanded mandate comes a commensurate responsibility to ensure the protection of such data and prevent its misuse or unauthorized exposure. Hence, The NRSE Act does not exempt the NRS from the application of the Nigeria Data Protection Act 2023. **Section 32(1)⁴⁴ of NRSE Act provides thus:** *"Without prejudice to the provisions of any other Act concerning data privacy or data protection, institutional information or communication, all internal information, communication, documents or memoranda of the service are confidential"*

The governing board of the Nigeria Revenue Service is vested with powers under section 4(2) of NRSEA, 2025⁴⁵ to make rules and issue regulations for "giving full effect to the provisions of this Act and for the due administration" including "compliance requirements and may include consequences for non-compliance in line with relevant laws." In exercise of the aforementioned powers, The NRS has in the past incorporated the requirement for confidentiality in its Human resources policies and process (HRPP).

To further strengthen the legal framework for the protection of taxpayer's data, the NRS establishment Act imposes a duty of secrecy on NRS officers and criminalises unauthorised disclosure. Section 33(1)(2) & (3) of the NRSE Act⁴⁶ imposes a strict duty of secrecy on all persons employed in the administration of the Act, requiring that all documents, returns, assessments, and information relating to a taxpayer's business, assets, liabilities and profits be treated as confidential. It prohibits unauthorized disclosure of such information except to persons authorized by the Service, by court order, or for purposes of this Act or any other tax law, with violations attracting a fine of up to N5,000,000 and/or 3 years imprisonment. The section also bars officials from being compelled to produce taxpayer information except in the course of tax-related legal proceedings in Nigeria. Equally, Section 32 of the NRSE Act⁴⁷ provides that all internal information, communications, documents and memoranda of the

Service are confidential, without prejudice to other data privacy laws. It prohibits any person from disclosing or attempting to disclose such institutional information, except where authorized by the Act, another law, an agreement, or by the Executive Chairman/Management. Breach attracts a penalty of up to N5,000,000 fine and/or 3 years imprisonment. With the foregoing provisions incorporated into the Nigeria Revenue Service (Establishment) Act, 2025, it is the writer's view that a legal framework has, to a considerable extent, been provided for the safeguarding and protection of taxpayer data in the custody of the NRS.

e) Nigeria Tax Administration Act, 2025

The objective of the Nigeria Tax Administration Act, 2025 is to provide a unified national legal framework for the efficient assessment, collection, and administration of taxes while safeguarding taxpayer rights and data. Sections 142 and 143 of the Nigeria Tax Administration Act, 2025 establish a comprehensive duty of confidentiality over taxpayer information. Section 142 provides thus: *“Without prejudice to the provisions of any other Act concerning data privacy, data protection and unlawful disclosure of taxpayer information, taxpayers’ information shall be confidential.”* This provides for a general rule that all taxpayers’ information shall be confidential without prejudice to other data protection laws. Section 143(1) imposes a direct obligation on any person employed in the administration of the Act to treat such information as secret and confidential, Section 143(1) NTAA provides thus: *“A person in an official duty or being employed for the administration of this Act or otherwise, that has access to taxpayer information shall regard and deal with such information as secret and confidential.”*

Section 143(2) of NTAA prohibits any person in possession of a taxpayer's documents, information or returns from communicating or revealing them to a third party without authorization or legal basis, while Section 143(3) of NTAA bars tax officials from being compelled to produce returns, documents or assessments, or to divulge information obtained in the course of their duties, except where necessary for instituting or prosecuting a tax-related offence in Nigeria. These provisions of the NTAA are all in line with the judicial pronouncement by a Nigerian Court in the case of **Anatogu v IMB (Nigeria) LTD (1985)**⁴⁸ the Courts held that *“institutions holding confidential data have a legal duty to protect it and that it can only be overridden by specific legal compulsions: a direct statutory command or an order of a court of competent jurisdiction.”*

f) Freedom of Information Act (FOIA) 2011:

The FOIA gives a right to access records held by public institutions, record may include taxpayer's data kept by the relevant tax authority of the three level of government. Section 1(1) of FOIA⁴⁹ provides that *“Notwithstanding anything contained in any other Act, law or regulation, the right of any person to access or request information, whether or not contained in any written form, which is in the custody or possession of any public official, agency or institution howsoever described, is established”* however section 14(1)(d) exempts taxpayer personal data related to its taxes. Section 14(1) (d) of FOIA⁵⁰ provide thus: *“Subject to subsection (2), a public institution must deny an application for information that contains personal information and information exempted under this subsection including (d) information required of any tax payer in connection with the assessment or collection of any tax unless disclosure is otherwise requested by the statute”*

The FOIA has provided another layer of protection for the taxpayer data privacy in Nigeria even though the scope of exemptions in tax matters has not been fully tested in Nigerian courts. It is necessary at this juncture to explain as discussed above under paragraph 2(c) of this article (international standard). The exemption provided against the release of taxpayer data and the

duty of secrecy impose on NRS is not absolute because of the provision of Section 33(4) of the NRSE Act which provides thus: *“The obligation as to secrecy imposed by this Act shall not prevent the disclosure of relevant information to an authorised officer of the Government of a country with which Nigeria has entered into any treaty, agreement or arrangement on tax matters.”*

Recently, amid growing public concern over data protection and transparency, civil society organisation Lawyers for Civil Liberties has invoked the Freedom of Information Act to demand disclosure of the Memorandum of Understanding signed between the Federal Inland Revenue Service (now Nigeria Revenue Service) and France’s Direction Générale des Finances Publiques⁵¹. In a letter dated 17 December 2025 to the Executive Chairman of FIRS and citing Sections 2, 5 and 21 of the FOI Act 2011, the group, led by National Coordinator Opatota Victor, stated that public access to the MoU is necessary to enable Nigerians to assess how the partnership aligns with national interests, protects taxpayer information, and preserves fiscal sovereignty. While commending FIRS for its efforts to modernize tax administration and adopt digital solutions, the organisation argued that releasing the agreement would strengthen public confidence in the tax system and clarify the scope of the FIRS-France partnership. The request was denied.⁵²

The Federal Inland Revenue Service has stated that its 10 December 2025 Memorandum of Understanding with France’s Direction Générale des Finances Publiques is confined to technical assistance and capacity building, and does not grant France access to Nigerian taxpayers’ data, digital systems, or operational infrastructure, with all existing Nigerian laws on data protection, cybersecurity, and sovereignty remaining fully applicable, the arrangement being described as advisory, non-intrusive, and under Nigeria’s control.⁵³

4.0 THE SOUTH AFRICAN FRAMEWORK FOR TAXPAYER DATA PROTECTION

a) The Constitution of the Republic of South Africa 1996: Section 14. the constitution of the Republic of South Africa 1996 provides for the Right of Privacy *“Everyone has the right to privacy, which includes the right not to have a. their person or home searched; b. their property searched; c. their possessions seized; or d. the privacy of their communications infringed.”* The right to privacy of citizens in South Africa has its origins in the common law, where it was recognized as part of the broader protection of human dignity and personality rights. However, its modern constitutional entrenchment was largely a reaction to the extensive state surveillance and intrusions that characterized the apartheid era. The framers of the 1996 Constitution sought to safeguard individuals from arbitrary interference with their private lives, family, home, and communications. Thus, the right to privacy in South Africa has evolved from common law principles into a constitutional guarantee aimed at protecting citizens from state overreach and ensuring respect for personal autonomy, family life, and human dignity.

The constitutional Court of South Africa on August 25, 2000 delivered its judgment *In Re Hyundai Motor Distributors (Pty) Ltd and Others v SMIT NO and OTHERS* 2001 (1) SA 545) where the Court decided on Right to privacy in terms of section 14 of Constitution of the Republic of South Africa Act 108 of 1996. It held thus: *“Right to privacy not relating solely to individual within his or her intimate space - When persons move beyond this established intimate core, they still retain right to privacy in social capacities in which they act - People in their offices, cars or on mobile telephones still retain right to be left alone by State unless certain conditions satisfied - Wherever person has ability to decide what he or she wishes to disclose to public and expectation that such decision will be respected is reasonable, right to privacy comes into play.”* The court further made pronouncement on the **Right to Privacy for Juristic Persons:**

The court confirmed that corporations and businesses (juristic persons) possess a right to privacy under the Bill of Rights, though it operates on a sliding scale.

Worthy of note also, is that the right to privacy under South African constitution is not an absolute or rigid entitlement, but rather a flexible and graduated right that varies in intensity according to context. The Constitutional Court of South Africa described it as existing on a continuum, radiating outward from the core of a person's most intimate sphere. At its centre lies a zone of intimate privacy that merits the highest protection. As one moves outward to family life, home, and public interactions, the expectation and scope of privacy correspondingly diminish. It therefore means that for the purpose of tax administration to generate revenue for the nation, the right of privacy can be tempered with. Section 36(1) & (2) of the S/A Constitution (Limitation of rights)⁵⁴

- 1. The rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, considering all relevant factors, including*
 - a. the nature of the right; b. the importance of the purpose of the limitation;*
 - c. the nature and extent of the limitation; d. the relation between the limitation and its purpose; and e. less restrictive means to achieve the purpose.*
- 2. Except as provided in subsection (1) or in any other provision of the Constitution, no law may limit any right entrenched in the Bill of Rights.*

From the above provision of the South African Constitution, it is unambiguous that any limitation on the right to privacy is permissible only if it is prescribed by a law of general application, pursues a legitimate and compelling public purpose such as national security, public safety, or the prevention and investigation of crime, and is proportionate to that purpose. This means the intrusion must be authorized by clear legislation, be necessary to achieve the stated public goal, and must not go further than is reasonably required, with no less restrictive means being available to attain the same objective.

b) Protection of Personal Information Act 4 (POPIA) 2013

The Protection of Personal Information Act, 2013 is a South African legislation enacted for the purpose of protecting the right to privacy of citizens by governing the processing of personal information. Section 1, chapter 1 of POPIA⁵⁵ clearly states the purpose of this legislation which is to give effect to the constitutional right to privacy by regulating the processing of personal information by responsible parties, subject to justifiable limitations that balance privacy with other rights such as access to information and the free flow of data. It sets minimum conditions for lawful processing in line with international standards, provides individuals with rights and remedies against unlawful processing, and establishes both voluntary and compulsory measures, including the Information Regulator, to promote, enforce, and uphold the rights protected by the Act.

It is interesting to note that the POPIA does not derogate from laws authorising processing including tax laws, it only makes such processing to be reasonable and justifiable. Section 37 chapter 4 of POPIA⁵⁶ provides to the extent that: the Regulator may, by notice in the Gazette, exempt a responsible party from compliance with any condition for the processing of personal information where it is satisfied that the public interest in such processing substantially outweighs any interference with a data subject's right to privacy, or where the processing confers a clear benefit on the data subject or a third party that similarly outweighs such interference. For purposes of this provision, "public interest" includes matters of national security, the prevention and prosecution of offences, important economic and financial interests of a public body, compliance with legal obligations, historical, statistical or research purposes,

and the exercise of freedom of expression. Any exemption so granted may be made subject to such reasonable conditions as the Regulator may impose. Where such conditions provided are violated, the Information Regulator established under the POPIA has powers to investigate, issue enforcement notices, and impose fines up to ZAR (South African Rand)10 million.⁵⁷

The Act under Sections 74-75 POPIA⁵⁸ provides a structured enforcement framework starting with complaints: any person may lodge a complaint with the Regulator, after which the Regulator decides whether to act, refer it to another body, or attempt settlement under Sections 76-80 POPIA.⁵⁹ If settlement fails, the Regulator may conduct pre-investigation and full investigation proceedings, issue warrants for search and seizure subject to legal safeguards and exemptions, and carry out assessments, issuing information notices and keeping parties informed under Sections 81-91 POPIA.⁶⁰ Matters that cannot be resolved may be referred to the Enforcement Committee for a hearing and decision under Sections 92-93 POPIA⁶¹, which can result in the issuance, variation, or cancellation of an enforcement notice under Sections 95-96 POPIA.⁶² Finally, affected parties have a right of appeal to a court under Sections 97-98 POPIA⁶³, and data subjects retain civil remedies to claim damages under Section 99 POPIA.⁶⁴ One can firmly state that the Protection of Personal Information Act No. 4 of 2013 is the legislation of the Republic of South Africa which give effect to the constitutional right to privacy, and by extension, provided for the protection of taxpayer information.

c) South African Revenue Service Act 34 of 1997:

The South African Revenue Service derives its core mandate and establishment from the South African Revenue Service Act 34 of 1997,⁶⁵ which constitutes it as the revenue authority of the Republic. However, the specific and extensive statutory powers conferred upon SARS to collect, access, and process personal and financial information for tax administration purposes are principally set out in Chapter 5 of the Tax Administration Act 28 of 2011. The effect of this legislative framework is that while the SARS Act provides for the existence and general functions of the Service, the Tax Administration Act operationalizes those functions by granting SARS far-reaching information-gathering powers necessary for the assessment, collection, and enforcement of tax.

SARS power to collect taxpayer data is rooted under Section 13(2)(b) of its establishment Act⁶⁶ which provides thus: “For the purposes of subsection (1) the Board— (b) is entitled to all relevant information concerning the administration of the revenue collecting system. excluding any information which is subject to a provision referred to in section 31.” The effect of this provision is to ensure that the Act operates subject to existing statutory duties of confidentiality and secrecy, and that it does not override, dilute or displace more specific prohibitions or regulatory frameworks governing the handling and disclosure of information held by the Commissioner. Accordingly, where other legislation imposes restrictions on disclosure, those restrictions shall continue to apply notwithstanding any provision of this Act. For avoidance of doubt, Section 31 SARSA 1997 (Protection of confidential information)⁶⁷ provides thus: *“Nothing in this Act affects provisions in other legislation prohibiting or regulating disclosure of information in the possession of the Commissioner”*

d) Tax Administration Act 28 of 2011:

the Tax Administration Act 28 of 2011 confers upon the South African Revenue Service enormous and far-reaching powers to collect taxpayer information for tax administration purposes. In terms of Section 46 TAA 2011⁶⁸, SARS may compel any person, whether a taxpayer or a third party, to submit "relevant material" which is broadly defined to include any information, document, or biometric data that is "foreseeably relevant" to tax administration. Further, Sections 40 and 45 of TAA 2011 empower SARS to conduct unannounced inspections

of business premises and to institute audits that may be random or risk-based. The Service may also summon individuals for oral interviews under Section 47 of TAA 2011, or institute formal inquiries under Section 50 TAA 2011 with powers akin to judicial proceedings. Most significantly, Section 63 TAA 2011 authorizes senior SARS officials to conduct searches of premises and seize documents or data, with or without a warrant, subject to either emergency or standard judicial conditions. Collectively, these provisions demonstrate that SARS possesses wide-ranging statutory authority to access, demand, and obtain taxpayer data by multiple means. More importantly, due to the significance and constitutional rooted right of privacy and by extension the protection of taxpayer data, Chapter 6 of the Tax Administration Act 28 of 2011 imposes a strict statutory duty of confidentiality on the South African Revenue Service and its officials in respect of all information acquired in the course of tax administration. Section 67 of the TAA 2011⁶⁹ establishes the general prohibition against disclosure, while Sections 68 and 69 of the TAA 2011⁷⁰ specifically create two distinct but overlapping categories of protected information, namely "SARS confidential information" and "taxpayer information". The effect of these provisions is to classify any information obtained or received by SARS in the course of performing its functions as secret. By so classifying it, the Act imposes a default rule of non-disclosure and restricts the use of such information solely to the purposes of tax administration. Consequently, SARS officials are legally barred from disclosing, disseminating, or using the information for any other purpose, unless disclosure is expressly authorized and falls within one of the limited exceptions set out elsewhere in Chapter 6 of the Act. This framework establishes a statutory veil of secrecy around all taxpayer data in SARS' possession.

The Act however provides limited and controlled exceptions to this rule: Section 70 allows disclosure to other entities such as government organs and foreign authorities for specified purposes; Section 71 of the TAA 2011⁷¹ permits disclosure in matters involving criminal offenses, public safety or environmental risks; Section 72 of the TAA protects against self-incrimination; Section 73 of the TAA 2011⁷² entitles a taxpayer to access their own records; and Section 74 of the TAA 2011⁷³ allows for the publication of names of offenders. The overall effect of Chapter 6 is to create a comprehensive confidentiality regime that safeguards taxpayer data, while balancing it against defined public interest and administrative exceptions.

e) Promotion of Access to Information Act 2 (PAIA) 2000⁷⁴.

The Act gives legislative effect to the constitutional right of access to information enshrined in Section 32 of the Constitution of the Republic of South Africa, 1996. The Act imposes a duty on both public and private bodies to grant access to any record in their possession upon request, unless such access is specifically and lawfully refused on grounds set out in PAIA itself. The effect of this is that the principle of openness applies broadly, and no entity is exempt merely by virtue of being a state institution or a private company. Accordingly, records held by the South African Revenue Service, being a public body, fall within the scope of PAIA and may be requested and accessed by any person, subject however to the limitations and refusal grounds provided for in the Act, including those relating to confidentiality and the protection of third-party information.

In furtherance of protection of taxpayer data, the PAIA exempt taxpayer data from public information and easily access. Section 35(1) of PAIA 2000 (Mandatory protection of certain records of South African Revenue Service)⁷⁵ provides thus: *"(1) Subject to subsection (2), the information officer of the South African Revenue Service, referred to in section 2(3), must refuse a request for access to a record of that Service if it contains information which was obtained or is held by that Service for the purposes of enforcing legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997*

(Act No. 34 of 1997). (2) A record may not be refused in terms of subsection (1) insofar as it consists of 20 information about the requester or the person on whose behalf the request is made.”

It can be deduced from the above provision that Section 35(1) of PAIA imposes a mandatory duty on SARS to refuse any request for access to records containing information obtained or held for the purposes of revenue collection. The effect of this is to provide strong statutory protection for taxpayer data in SARS’ possession and to preserve the confidentiality and integrity of tax administration. However, subsection (2) qualifies this general rule by providing that SARS may not refuse access where the record consists of information about the requester or the person on whose behalf the request is made. In this way the provision balances the protection of third-party taxpayer information with the right of a taxpayer to access their own records.

In what looks like a spoke in the wheel of taxpayer data protection which constitutes a critical weakness in the taxpayer data protection framework, section 46 of PAIA 2000⁷⁶ creates a "public interest override" when it stated that: Notwithstanding any other confidentiality ground in Chapter 2 of PAIA, an information officer must grant access to a record if two conditions are met: First, disclosure would reveal evidence of either (a) a substantial contravention of, or failure to comply with, the law, or (b) an imminent and serious public safety or environmental risk. Second, the public interest in disclosing the record must clearly outweigh the potential harm that would otherwise justify refusal under the relevant exemption provision. The researcher is of the opinion that this provision allows access to otherwise protected records, including confidential government information and by wider extension taxpayer data where disclosure is necessary to expose serious illegality or danger and where the benefit to the public clearly outweighs the harm of disclosure.

Recently, the Constitutional Court of South Africa delivered its Judgement on 30 May 2022 on the interpretation of the constitutionality or otherwise of Section 35 and 46 of PAIA in the case of **Arena Holdings (Pty) Ltd v SARS (2023)**⁷⁷: the brief facts of the case are as follows: In 2019, journalist Warren Thompson, Arena Holdings and AmaBhungane applied under PAIA for access to former President Jacob Zuma’s tax records following allegations in The President’s Keepers. SARS refused, relying on the confidentiality provisions in sections 35(1) and 46 of PAIA and sections 67 and 69 of the TAA. The applicants challenged this in the High Court, arguing the blanket ban unjustifiably limited their rights to access to information and freedom of expression where public interest was involved. The High Court declared the provisions unconstitutional to that extent and ordered disclosure. SARS, the Ministers and Mr Zuma opposed confirmation, contending the secrecy regime was essential to protect taxpayer privacy and tax compliance. In a majority judgment, the Constitutional Court confirmed the High Court’s declaration of invalidity. It held that the absolute prohibition in s 35(1) of PAIA, reinforced by ss 67(4) and 69(2) of the TAA, failed the s 36 limitation test because it immunised all taxpayer information from disclosure regardless of context, and could not be justified as necessary for taxpayer compliance or privacy. The Court found that the PAIA “public-interest override” already provides a narrow, checked mechanism for lifting confidentiality where disclosure would reveal a substantial contravention of the law or serious risk and is in the public interest, and that taxpayer records should not be excluded from it. The declaration of invalidity was suspended for 24 months to allow Parliament to remedy the defect, with a reading-in of “35(1)” into s 46 of PAIA and a new subsection into the TAA to permit disclosure where access is granted under PAIA. The Court set aside the High Court’s direct order for release of Mr Zuma’s records and instead referred the PAIA request back to SARS for reconsideration under

the corrected law. Costs for the confirmation proceedings were awarded against SARS and the two Ministers.

5.0 COMPARATIVE ANALYSIS

a) Constitutional Foundation of Privacy

NRS – Nigeria: In Nigeria, the right to privacy is constitutionally guaranteed, but the courts have traditionally read it narrowly.⁷⁸ Early decisions limited it mainly to the home, personal correspondence, and telephone communications. More recent jurisprudence has begun to broaden that scope to cover personal data, recognizing that privacy in the digital age must extend to information held by the state and private actors. However, the text itself does not expressly mention taxpayer information. Because privacy is treated as a qualified right, it may be limited where the government can show a legitimate public purpose such as tax administration, revenue collection, and public interest.

SARS – South Africa: South Africa’s constitutional protection of privacy is broader from the outset. It covers not only the home and communications, but also a person’s body, property, possessions, and personal autonomy. The courts⁷⁹ have described it as a “sliding scale” right strongest in intimate spaces, but still present in offices, vehicles, and digital communications. This means individuals retain a reasonable expectation of privacy even in their professional and financial affairs. Like in Nigeria, the right is not absolute. It can be limited, but only where the limitation is reasonable, lawful, and justifiable in an open and democratic society, with proper regard to proportionality.

Comparison: The key difference is in breadth and flexibility. South Africa starts with an expansive constitutional guarantee and a clear test for when it may be limited. Nigeria starts with a narrower textual guarantee that courts have had to interpret expansively to keep pace with technology. Both systems, however, accept that taxpayer data may be collected for revenue purposes, provided it is done lawfully and with adequate safeguards.

b) Primary Data Protection Legislation:

NRS – Nigeria: Nigeria’s data protection framework is anchored by a comprehensive data protection law and its accompanying regulation. The law applies to the Nigeria Revenue Service in the same way it applies to any other data controller that processes personal information. It sets out lawful grounds for processing, including where it is necessary for the performance of a public function such as tax administration. The law also imposes clear security obligations, requiring measures like encryption, data minimization techniques, and regular risk assessments to protect the data held. Oversight is vested in the national data protection authority, which has powers to investigate breaches and impose financial penalties that scale with the size and importance of the organization. For data transferred outside the country, the law requires that the receiving jurisdiction provide an adequate level of protection or that appropriate safeguards are put in place.

SARS – South Africa: South Africa’s framework is built around its dedicated data protection Act, which gives effect to the constitutional right to privacy. The law sets out core principles for lawful processing and applies to all public and private bodies, including the revenue authority. It recognizes that tax administration serves an important public interest, and therefore allows the data protection regulator to grant exemptions where that public interest clearly outweighs privacy concerns. The regulator is empowered to investigate complaints, issue enforcement notices, and levy substantial administrative fines. Because the law has been in force for longer, there is more regulatory guidance and case practice on how it applies to government.

Comparison: Both countries now have modern, principle-based data protection laws with independent regulators and real enforcement powers. South Africa’s regime is more mature

and has an explicit mechanism for balancing tax enforcement with privacy. Nigeria's framework is newer, closely aligned with international best practice, and introduces stricter timelines for breach notification and a stronger emphasis on technical security measures. In both cases, the revenue authorities must comply with the same data protection standards as other institutions, even as they exercise broad powers for tax purposes.

c) Tax Authority Secrecy and Disclosure Powers:

NRS – Nigeria: Nigerian law places a strict duty of secrecy on revenue officers. Any unauthorized disclosure of taxpayer information is treated as a criminal offense punishable by fine and imprisonment. All internal NRS records are also classified as confidential. The main exception is for international cooperation: The Service may share taxpayer data with other countries where Nigeria has a tax treaty or agreement. Outside of that, public access to taxpayer data is generally barred unless another law specifically allows it.

SARS – South Africa: South Africa operates a detailed secrecy regime under its tax administration law. All information obtained by SARS in the course of its duties is considered confidential by default. The law then sets out clear, codified exceptions for disclosure to other government bodies, foreign tax authorities under exchange agreements, for criminal investigations, and to allow taxpayers to access their own records. A separate law also reinforces the duty to protect confidential information held by SARS.

Comparison: Both countries default to secrecy and impose criminal penalties for breaches. South Africa's approach is more detailed, with explicit categories for when disclosure is permitted, including a clear framework for international exchange. Nigeria's approach relies on a broad secrecy duty with specific carve-outs for treaty partners, and otherwise restricts access.

d) Public Access to Information v Taxpayer Confidentiality:

NRS – Nigeria: Nigeria's access to information law gives the public a general right to request records held by government bodies. However, it specifically exempts taxpayer information collected for tax assessment and collection. The exemption is applied strictly. A recent attempt by a civil society group to obtain the NRS-France cooperation agreement under this law was denied, showing that taxpayer-related documents are largely shielded from public disclosure even where transparency is sought.

SARS – South Africa: South Africa's law also requires SARS to refuse access to records held for revenue purposes. But it makes two important distinctions. First, taxpayers can access their own records. Second, the law includes a "public interest override." This means that if disclosure is needed to expose serious wrongdoing or a serious risk, and the public interest outweighs the harm, access can be granted. The courts have confirmed this override applies even to taxpayer data, so an absolute ban on disclosure is no longer valid.

Comparison: Both countries protect taxpayer data from general public access. The key difference is flexibility. South Africa now allows for limited disclosure where there is a strong public interest, backed by court authority. Nigeria's exemption is absolute, with no public interest test, making it much harder to access agreements or information about how taxpayer data is being used, even for accountability purposes.

e) Enforcement and Oversight Architecture:

NRS – Nigeria: Nigeria operates a dual oversight system. The national data protection authority enforces the data protection law and can investigate breaches, issue penalties, and mandate reporting of security incidents within 72 hours. Within NRS, the governing board can issue compliance regulations, and the Service itself must appoint data protection officers and

publish privacy policies. This means NRS has broad powers to collect and process taxpayer data, but it must answer to an independent regulator and meet clear internal governance requirements.

SARS – South Africa: South Africa also uses dual oversight. The Information Regulator enforces the data protection Act with powers to investigate, conduct searches, issue enforcement notices, and levy fines. At the same time, SARS has extensive powers under tax law to demand records, carry out inspections, conduct interviews, and execute searches and seizures. These powers are balanced by a strong confidentiality regime that limits how taxpayer information can be handled and shared.

Comparison: Both countries give their revenue authorities wide data-collection powers, but place them under independent data regulators. South Africa’s regulator has more mature and detailed enforcement tools. Nigeria’s regulator is newer, but introduces stricter requirements like mandatory 72-hour breach notification.

6.0 CHALLENGES LIMITING EFFECTIVE TAXPAYER DATA PROTECTION IN BOTH NIGERIA AND SOUTH AFRICA

a) **Cybersecurity Vulnerability:** A major shared challenge for Nigeria and South Africa is cybersecurity failure in tax administration. In South Africa, the Tax Ombud’s October 2025 report found nearly 16,000 e-filing accounts were hijacked through phishing and weak authentication, with tax practitioners most affected. SARS refunded over R21 million to victims.⁸⁰ The report blamed poor authentication, slow fraud response, and possible insider involvement, and recommended 2FA, biometrics, and real-time alerts. A May 2026 claim of a major SARS breach was denied by SARS as misinformation, but highlighted how reputational damage from alleged breaches can match that of actual ones. In Nigeria, risks are similar but less documented: legacy IT systems, weak cloud configurations, phishing, and ransomware are key threats. Capacity is limited, with too few certified cybersecurity professionals and unstable power forcing reliance on insecure infrastructure. The NDPC’s largest fine to date, ₦555.8 million against Fidelity Bank in August 2024, shows that even major institutions reporting data to the NRS remain vulnerable.⁸¹

b) **Expanding Data-Collection Powers and the Proportionality Problem:** Both Nigeria and South Africa have broadened state powers to collect taxpayer data in the same reform cycle, but rely on general proportionality principles rather than tax-specific limits to prevent abuse. Nigeria’s NTAA now requires financial institutions to report high-value transactions and counterparty identities. The NRS’ reach has also expanded to cover remote workers’ foreign income, crypto assets, and non-resident digital services. The General Application and Implementation Directive bars “fishing expeditions,” but its effectiveness depends on the NDPC’s enforcement capacity, which remains weak. Public backlash over the NRS-France MoU, despite NRS’ assurance that it involved only technical assistance, shows that credibility now hinges on transparency as much as legal authority. South Africa faces the same issue: SARS’ third-party data matching and automated risk-scoring raise questions about when legitimate revenue-risk aggregation becomes financial surveillance. While POPIA’s purpose-limitation and data-minimisation rules apply to SARS, South Africa lacks a tax-specific instrument defining what “proportionate” collection by a revenue authority entails, unlike Nigeria’s Directive.

c) **Institutional Capacity and Enforcement Gaps:** The effectiveness of both frameworks depends on regulator capacity, but both the NDPC and South Africa’s Information Regulator (SAIR) show a pattern of bold announcements with inconsistent follow-through. In Nigeria, the NDPC has imposed major fines, including ₦555.8 million on Fidelity Bank in 2024 and a \$220 million penalty on Meta with the FCCPC, later reduced and then fully waived

in a confidential October 2025 settlement.⁸² This reversal undermines deterrence, especially as the NRS now relies on financial institutions to securely report taxpayer data under the NTAA. In South Africa, the Information Regulator has fined government departments and targeted global platforms, and plans tougher action in its 2025/26 plan. However, its largest fine against the Department of Basic Education was overturned in December 2025,⁸³ showing ongoing uncertainty around the scope of “personal information.” Crucially, neither regulator has yet taken enforcement action against a revenue authority’s own tax-data processing, leaving the area most central to taxpayer protection largely untested.

d) **Digital Literacy, Awareness and Taxpayer Trust:** Both frameworks assume taxpayers can understand and exercise their data-protection rights, but evidence in both countries shows this is not yet the case. In Nigeria, surveys across all six zones show most taxpayers expect benefits from automated tax systems, yet over half doubt current laws adequately protect data privacy. Respondents cited unclear guidelines, weak enforcement, and low trust as key problems. Wider commentary also points to low tax morale, poor digital/financial literacy, unreliable power and networks, English-only e-tax platforms despite use of Hausa, Yoruba, Igbo and Pidgin, and limited access for persons with disabilities as barriers to real digital inclusion. In South Africa, the Tax Ombud found low digital-security awareness, weak/reused passwords, phishing vulnerability, and distrust of police discouraged reporting, all of which fuelled the e-filing hijacking problem. In both countries, lack of trust undermines compliance: taxpayers resist digital platforms, fall for tax-related phishing, and delay reporting breaches, making it harder for revenue authorities to detect and contain incidents.

e) **Cross-Border Data Flows and International Tax Cooperation:** Both countries must balance two conflicting goals: wider tax-information exchange to combat evasion, and strict privacy protections that limit data flows. Nigeria’s Data Protection Act restricts cross-border transfers unless adequacy or safeguards exist, and the NDPC was still reviewing compliance mechanisms as of mid-2026. Yet Nigeria’s Common Reporting Standard participation and the partially disclosed NRS-DGFIP MoU mean large volumes of financial data now move under tax-treaty rules, which are not fully aligned with the Act’s transfer regime. South Africa faces the same mismatch. POPIA’s Section 72 requires adequate protection abroad, but SARS’ Common Reporting Standard and bilateral exchanges operate under OECD confidentiality standards, not POPIA’s conditions. Neither the NDPC nor South Africa’s Information Regulator has issued guidance reconciling general data-transfer rules with treaty-based tax exchanges, leaving taxpayers, banks, and revenue authorities without clear standards for “adequate protection” in a tax context.

f) **Artificial Intelligence and Taxpayer Profiling:** An emerging challenge for both countries is the use of AI and machine learning for taxpayer risk profiling. AI promises more dynamic risk assessment than traditional rule-based systems, but it relies on large, often opaque datasets that can embed historical bias. When models operate as “black boxes,” taxpayers cannot see why they were flagged for audit, undermining transparency and due-process requirements in both Nigeria’s and South Africa’s data protection laws. Nigeria’s NRS is reportedly testing analytics and ML for fraud detection with support from ATAF and UNDP, but the NDPA does not yet require bias audits, model documentation, or a right to human review of adverse automated decisions. Similarly, SARS has expanded automated verification and risk-scoring, and the Tax Ombud linked weak fraud-detection algorithms to prolonged e-filing hijacking. Yet POPIA also lacks tax-specific safeguards for automated profiling. In both jurisdictions, current data protection laws have not kept pace with AI-driven tax enforcement.

7.0 WAY FORWARD:

a) Cybersecurity Vulnerability: Both countries should mandate compulsory 2FA, biometric verification, and real-time alerts across all taxpayer portals, and establish dedicated Cybersecurity Operations Centres within NRS and SARS for 24/7 threat detection and rapid response. This must be paired with annual independent security audits of financial institutions and service providers, targeted training to close the skills gap, and for Nigeria, investment in secure cloud infrastructure with backup power to reduce reliance on vulnerable systems. A clear public breach communication protocol is also needed to manage reputational damage from both real and alleged incidents.

b) Expanding Data-Collection Powers and the Proportionality Problem: The solution is to move beyond general principles and issue tax-specific subsidiary regulations under the NDPA and POPIA that define exactly what data NRS and SARS can collect, for what purpose, and for how long, with explicit bans on “fishing expeditions.” Data protection regulators should be empowered to pre-approve large-scale collection programs, and all cross-border agreements like MoUs must be published with a public impact assessment before implementation to build trust that expanded powers are not being used for mass surveillance.

c) Institutional Capacity and Enforcement Gaps: Regulators need ring-fenced funding, dedicated tax-data units, and binding rules that prohibit confidential waivers of major fines without public disclosure of terms and rationale. Both the NDPC and Information Regulator must prioritize their first enforcement actions against revenue authorities themselves to test and legitimize the framework, while formalizing MOUs with tax authorities and competition bodies to ensure consistent follow-through. Credibility will come from predictable, transparent enforcement, not just high-profile announcements.

d) Digital Literacy, Awareness and Taxpayer Trust: Governments should roll out national, multi-language digital tax literacy campaigns delivered via USSD, radio and community channels, covering phishing, password security, and taxpayer rights in local languages beyond English. E-filing platforms must be made accessible, mobile-first, disability-friendly, and revenue authorities should create non-police, anonymous channels for reporting suspected fraud. Publishing annual transparency reports on breaches and remediation will help rebuild trust and encourage prompt reporting, which is critical for containing incidents.

e) Cross-Border Data Flows and International Tax Cooperation: The NDPC and Information Regulator must issue joint guidance reconciling Common Reporting Standard and tax-treaty exchanges with NDPA and POPIA’s adequacy and safeguard requirements, and develop standard contractual clauses for all tax MoUs that embed data minimization and taxpayer redress. A public register of all jurisdictions receiving tax data, with the legal basis for each transfer, should be maintained. This will provide clarity to banks, taxpayers, and revenue authorities on what “adequate protection” means in a tax context.

f) Artificial Intelligence and Taxpayer Profiling: NRS and SARS should be required to document all AI/ML risk models, conduct mandatory bias audits, and maintain logs of data provenance before deployment. Taxpayers must have a statutory right to request a human-reviewed explanation for any adverse automated decision, such as audit selection. An independent AI ethics board within each revenue authority, with regulator approval needed for new models, will ensure that the move to dynamic profiling does not erode transparency and due process.

8.0 CONCLUSION

Nigeria and South Africa illustrate two trajectories toward the same goal: enabling revenue authorities to use data for compliance while protecting the constitutional right to privacy. Both jurisdictions have moved from fragmented rules to comprehensive regimes that recognize confidentiality, impose penalties for breaches, and accommodate international information exchange. Yet law alone is insufficient. The analysis reveals critical convergence on principles, but divergence in practice. Nigeria's framework is new and expansive, but its effectiveness hinges on building NDPC capacity, clarifying the scope of Section 37, and making data-collection powers proportionate and transparent. South Africa benefits from a tested regulator and judicial checks, but must address cybersecurity vulnerabilities and ensure that broad SARS powers under the TAA remain subject to POPIA's safeguards. Across both countries, trust is the missing variable. Taxpayers who doubt security, proportionality, or fairness will resist digital systems, fall prey to phishing, and withhold cooperation—undermining the very compliance goals the reforms seek. The way forward requires four shifts: 1) codifying tax-specific data-protection standards; 2) investing in cybersecurity and institutional capacity; 3) aligning cross-border tax cooperation with domestic privacy law; and 4) embedding transparency, literacy, and human oversight into AI-driven tax administration. In an era where data is the currency of tax administration, the legitimacy of NRS and SARS will depend not only on what they can collect, but on how convincingly they can prove they can protect it.

¹ R. Zambrano, S.D. De-Saralde, A.Barreix and B. Martin “*The Future of Tax Administrations Lies in the Intelligence Generated by Big Data*” <https://www.iadb.org/en/blog/modernization-state/fiscal-management/future-tax-administrations-lies-intelligence-generated-big-data> Accessed on 19th May, 2026

² Peter Hongler, International Taxation in an Era of Digital Disruption (IBFD 2020) 112.

³ M.J Garde, Z. Manatta, M. Estevão and R. Arezki OECD “*Global forum on transparency and exchange of information for tax purpose: Model Manual on Exchange of Information for Tax Purposes*” Pg. 5 <https://www.oecd.org/content/dam/oecd/en/networks/global-forum-tax-transparency/eoi-manual-en.pdf> Accessed on 20th May, 2026.

⁴The guardian news online: “*Tax Reforms: Nigeria Revenue Service accredits Afri Invoice as system integrator*” <https://guardian.ng/news/tax-reforms-nigeria-revenue-service-accredits-afri-invoice-as-system-integrator/> Accessed on 20th May, 2026.

⁵KPMG “South Africa: Tax authority confirms multi-year e-invoicing and digital reporting reform” <https://kpmg.com/us/en/taxnewsflash/news/2026/02/south-africa-tax-authority-confirms-multi-year-e-invoicing-digital-reporting-reform.html> accessed on 28th July, 2026

⁶ OECD (2020), *Tax Administration 3.0: The Digital Transformation of Tax Administration*, Pg. 24 OECD Publishing, Paris, <https://doi.org/10.1787/ca274cc5-en>. Pg. 24 accessed 28th July, 2026.

⁷ Law insider dictionary ‘taxpayer data meaning’ <https://www.lawinsider.com/dictionary/taxpayer-data> accessed 29th July, 2026.

⁸ The Tax Law Centre at NYU Law ‘Understanding Taxpayer Privacy Protections Under Section 6103 and Related Statutes’ Feb 10, 2025. <https://medium.com/@taxlawcenter/understanding-taxpayer-privacy-protections-under-section-6103-and-related-statutes-8ad8ef26efee> accessed on 6th July, 2026

⁹ L Bygrave, *Data Privacy Law: An International Perspective* 2nd edn, OUP 2014 pg.104 also available at <https://dokumen.pub/data-privacy-law-an-international-perspective-9780199675555.html> accessed 29th July, 2026.

¹⁰ Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217A(III) art 12. Available at <https://www.un.org/en/about-us/universal-declaration-of-human-rights> accessed on 27th July, 2026

¹¹ International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 art 17.

¹² African Charter on Human and Peoples’ Rights (adopted 27 June 1981, entered into force 21 October 1986) (1982) 21 ILM 58 art 4, 5, & 6 available at <https://africanlii.org/en/akn/aa-au/act/charter/1981/human-and-peoples-rights/eng@1981-06-27> accessed on 27th July, 2026

¹³ <https://www.diplomacy.edu/blog/what-is-the-malabo-convention/> Accessed on 29th July, 2026

¹⁴ African Union Convention on Cybersecurity and Personal Data Protection (adopted 27 June 2014) also known as the **Malabo Convention**. art 8. <https://ulii.org/en/akn/aa-au/act/convention/2014/cyber-security-and-personal-data-protection/eng@2014-06-27> Accessed on 29th July, 2026

-
- ¹⁵ Nose M, Pierri N and Honda J, Leveraging Digital Technologies in Boosting Tax Collection (IMF Working Paper WP/25/89, International Monetary Fund 2021) <<https://www.imf.org/-/media/files/publications/wp/2025/english/wp25089-print-pdf.pdf>> accessed 28th July, 2026
- ¹⁶ Aishatu I. 'The Impact of Data Breaches on Tax Compliance Behavior: Evidence from Digital Taxpayers' (2025) 28(2) World Journal of Advanced Research and Reviews 1107, 1112. Available at https://www.researchgate.net/publication/397754614_The_Impact_of_Data_Breaches_on_Tax_Compliance_Behavior_Evidence_from_Digital_Taxpayers accessed 30th July, 2026
- ¹⁷ Visser A, 'Deep Flaws In SARS's Systems, OTO Investigation Finds' Moonstone (online, 6 October 2025) <https://www.moonstone.co.za/deep-flaws-in-sarss-systems-oto-investigation-finds/> accessed on 30th July, 2026
- ¹⁸ Ibid immediate footnote 15.
- ¹⁹ Osundolire O, Muse-Sadiq A and Oguntuase O, 'Nigeria's New Tax Regime: Income tracking powers of tax authorities and data protection concerns' (Banwo & Ighodalo, 11 March 2026) < <https://www.banwo-ighodalo.com/grey-matter/nigerias-new-tax-regime-income-tracking-powers-of-tax-authorities-and-data-protection-concerns/>> accessed 29th July, 2026
- ²⁰ Chibuzor Emejor and Samuel Ogidan, 'FIRS, France Tax MoU Threat to Nat'l Security — Northern Elders' Independent Nigeria (online, 15 December 2025) <https://independent.ng/firs-france-tax-mou-threat-to-natl-security-northern-elders/> accessed 29th July, 2026.
- ²¹ OECD Common Reporting Standard and Automatic Exchange of Information (CRS/AEOI) https://www.oecd.org/en/publications/consolidated-text-of-the-common-reporting-standard-2025_055664b1-en.html accessed on 30th July, 2026
- ²² Sovereign Group, 'CRS 2.0 and CARF Explained: What the New Global Reporting Rules Mean (How does the Common Reporting Standard work today?)' Sovereign Group (online, nd) <https://www.sovereigngroup.com/news/explainer-changes-to-the-global-tax-transparency-framework-crs-2-0-and-the-carf/> accessed 30 July 2026
- ²³ KPMG, '2025 Update to the OECD Model Tax Convention' KPMG (online, 2025) <https://kpmg.com/be/en/insights/my-tax-compass/corporate-tax-insights/2025-update-to-the-oecd-model-tax-convention.html> accessed 30 July 2026
- ²⁴ The Constitution of Federal Republic of Nigeria (As Amended) 1960 S.34
- ²⁵ The Constitution of Federal Republic of Nigeria (As Amended) 1979 S.34
- ²⁶ The Constitution of Federal Republic of Nigeria (As Amended) 1979 S.37
- ²⁷ Solove, Daniel, J. Understanding Privacy. Cambridge, MA: Harvard University Press, 2008.
- ²⁸ Olomjobi, Yinka, Right to Privacy in Nigeria (October 31, 2017). Available at SSRN: <https://ssrn.com/abstract=3062603> or <http://dx.doi.org/10.2139/ssrn.3062603>
- ²⁹ Ibid
- ³⁰ Nigeria Data Protection Act 2023, s 2(1) provides thus: "This Act shall apply to the processing of personal data, whether by automated means or not. (2) This Act shall apply, where the- (a) data controller or data processor is domiciled in, resident in, or operating in Nigeria; (b) processing of personal data occurs within Nigeria; or (c) the data controller or the data processor is not domiciled in, resident in, or operating in Nigeria, but is processing personal data of a data subject in Nigeria"
- ³¹ Nigeria Data Protection Act 2023, s 25.
- ³² Nigeria Data Protection Act 2023, s 24.
- ³³ Nigeria Data Protection Act 2023, s 32.
- ³⁴ Nigeria Data Protection Act 2023, s 38.
- ³⁵ Nigeria Data Protection Act 2023, s 39.
- ³⁶ National Information Technology Development Agency Act 2007. S.6(a) & (b)
- ³⁷ The Nigeria Data Protection Regulation (NDPR) 2019, Paragraph 1.1 Available at <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf> accessed on 3rd August, 2026
- ³⁸ The Nigeria Data Protection Regulation (NDPR) 2019, Paragraph 1.2 Available at <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf> accessed on 3rd August, 2026
- ³⁹ The Nigeria Data Protection Regulation (NDPR) 2019, Paragraph 2.11. Available at <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf> accessed on 3rd August, 2026
- ⁴⁰ The Nigeria Data Protection Regulation (NDPR) 2019, Paragraph 2.5 Available at <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf> accessed on 3rd August, 2026
- ⁴¹ The Nigeria Data Protection Regulation (NDPR) 2019, Paragraph 4.1(4) Available at <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf> accessed on 3rd August, 2026
- ⁴² The Nigeria Data Protection Regulation (NDPR) 2019, Paragraph 4.3 Available at <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf> accessed on 3rd August, 2026
- ⁴³ Nigeria Revenue Service (Establishment) Act 2025, s 4(1)(l)(m)(q).
- ⁴⁴ Nigeria Revenue Service (Establishment) Act 2025, s 32(1).
- ⁴⁵ Nigeria Revenue Service (Establishment) Act 2025, s 4(2).
- ⁴⁶ Nigeria Revenue Service (Establishment) Act 2025, s 33(1)(2) & (3)
- ⁴⁷ Nigeria Revenue Service (Establishment) Act 2025, s 32(1) & (2)
- ⁴⁸ Analogue v IMB (Nigeria) LTD (1985)1 NWLR (pt.1) 45,

-
- ⁴⁹ Freedom of Information Act 2011 (was passed into law on May 28, 2011) s.1(1) Available at <https://ncdmb.gov.ng/wp-content/uploads/2025/12/freedom-of-information-act.pdf> Accessed on 4th August, 2026
- ⁵⁰ Freedom of Information Act 2011 (was passed into law on May 28, 2011) s.14(1)(d) Available at <https://ncdmb.gov.ng/wp-content/uploads/2025/12/freedom-of-information-act.pdf> Accessed on 4th August, 2026
- ⁵¹ Samson Akintaro, 'FIRS-France MoU: Lawyers Invoke FOI to Access Details of Agreements' Naira metrics (18 December 2025) <https://nairametrics.com/2025/12/18/firs-france-mou-lawyers-invoke-foi-to-access-details-of-agreements/> accessed 13 August 2026
- ⁵² Samson Akintaro, 'FIRS-France MoU: Lawyers Invoke FOI to Access Details of Agreements' Naira metrics (18 December 2025) <https://nairametrics.com/2025/12/18/firs-france-mou-lawyers-invoke-foi-to-access-details-of-agreements/> accessed 13 August 2026
- ⁵³ Harrison Edih, 'Experts Differ as FIRS Claims MoU with France Won't Compromise Taxpayers' Data' International Centre for Investigative Reporting (ICIR) (15 December 2025) <https://www.icirnigeria.org/experts-kick-as-firs-claims-mou-with-france-wont-compromise-taxpayers-data/> accessed 12 August 2026
- ⁵⁴ The Constitution of Republic of South Africa, s. 36(1) & (2)
- ⁵⁵ Protection of Personal Information Act 4, of 2013 s. 1, chapter 1, available at <https://popia.co.za/protection-of-personal-information-act-popia/chapter-10/> accessed on 3rd August, 2026
- ⁵⁶ Protection of Personal Information Act 4, of 2013 s. 37, chapter 4, available at <https://popia.co.za/protection-of-personal-information-act-popia/chapter-10/> accessed on 3rd August, 2026
- ⁵⁷ Protection of Personal Information Act 4, of 2013 s. 109, chapter 11
- ⁵⁸ Protection of Personal Information Act 4, of 2013 s. 74-75, chapter 10
- ⁵⁹ Protection of Personal Information Act 4, of 2013 s. 76-80, chapter 10
- ⁶⁰ Protection of Personal Information Act 4, of 2013 s. 81-91, chapter 10
- ⁶¹ Protection of Personal Information Act 4, of 2013 s. 92-93. chapter 10
- ⁶² Protection of Personal Information Act 4, of 2013 s. 95-96. chapter 10
- ⁶³ Protection of Personal Information Act 4, of 2013 s. 97-98. chapter 10
- ⁶⁴ Protection of Personal Information Act 4, of 2013 s. 99. chapter 10
- ⁶⁵ South African Revenue Service Act 34 of 1997 Available at https://www.gov.za/sites/default/files/gcis_document/201409/a34-97.pdf Accessed on 5th of August, 2026
- ⁶⁶ South African Revenue Service Act 34 of 1997. S. 13(2)(b)
- ⁶⁷ South African Revenue Service Act 34 of 1997. S. 31
- ⁶⁸ Tax Administration Act 28 of 2011, s.46 Available at https://www.gov.za/sites/default/files/gcis_document/201409/a282011.pdf Accessed on 7th August, 2026.
- ⁶⁹ Tax Administration Act 28 of 2011, s.67
- ⁷⁰ Tax Administration Act 28 of 2011, s.68 & 69
- ⁷¹ Tax Administration Act 28 of 2011, s.68 & 71
- ⁷² Tax Administration Act 28 of 2011, s.68 & 73
- ⁷³ Tax Administration Act 28 of 2011, s.68 & 74
- ⁷⁴ Promotion of Access to Information Act 2 (PAIA) 2000 Available https://www.gov.za/sites/default/files/gcis_document/201409/a2-000.pdf accessed on 6th August, 2026.
- ⁷⁵ Promotion of Access to Information Act 2 (PAIA) 2000, s.35
- ⁷⁶ Promotion of Access to Information Act 2 (PAIA) 2000, s.46
- ⁷⁷ Arena Holdings (Pty) Ltd v SARS CCT365/21 (2023) Available at <https://www.concourt.org.za/index.php/judgement/511-arena-holdings-pty-limited-t-a-financial-mail-and-others-v-south-african-revenue-service-and-others-cct365-21> accessed on 30th July, 2026.
- ⁷⁸ Emerging Market Telecommunication Services v Barr Godfrey Nya Eneye (2018) LPELR-46193
- ⁷⁹ Re Hyundai Motor Distributors (Pty) Ltd and Others v SMIT NO and OTHERS 2001 (1) SA 545
- ⁸⁰ Visser A, 'Deep Flaws In SARS's Systems, OTO Investigation Finds' Moonstone (online, 6 October 2025) <https://www.moonstone.co.za/deep-flaws-in-sarss-systems-oto-investigation-finds/> accessed on 30th July, 2026
- ⁸¹ Soonest Nathaniel 'Fidelity Bank was found to have breached the Nigeria Data Protection Regulation (NDPR) of 2019 and the Nigeria Data Protection (NDP) Act of 2023.' Channels TV, August 21st, 2024. Available at <https://www.channelsstv.com/2024/08/21/fidelity-bank-fined-n555-8m-by-ndpc-for-data-breach/> accessed on 8th August, 2026
- ⁸² Bello T, 'Violation: Tribunal Upholds FCCPC's \$220 Million Fine Against Meta/WhatsApp' (Federal Competition and Consumer Protection Commission, 2026) <https://fccpc.gov.ng/violations-tribunal-upholds-fccpcs-220-million-fine-against-meta-whatsapp/> accessed 9 August 2026
- ⁸³ South Africa Broadcasting Corporation (SABC)/Channel Africa-- 'SA Information Regulator fines Education department for non-compliance' December 24th, 2024, available at <http://web.sabc.co.za/sabc/home/channelafrica/news/details?id=cffb4a79-1eff-4bcc-981a-28c8a82da22b&title=SA+Information+Regulator+fines+Education+department+for+non-compliance> accessed on 11th August, 2026

