International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 05-06-2026, Accepted: 05-07-2026, Published: 20-07-2026
Volume 12, Issue 3, 2026, Page No. 139-146

Public registers and private rights: A critique of data safeguards in Nigeria's PSC Regulations 2022 and the UK persons with significant control framework

Oyinkare Omemu-Harrison[1], Jonathan Ekperusi[2]
[1] Lecturer & Researcher, Faculty of Law, Niger Delta University, Bayelsa, Nigeria
[2] Dean, Faculty of Law, Southern Delta University, Delta, Nigeria

Abstract
Corporate transparency and individual privacy are core tenets of modern democratic governance. They are constitutionally and legislatively recognised. Beneficial ownership disclosure most poignantly illustrates the intersection of the two values when a public register mandates disclosure of personal information by Persons with Significant Control (PSCs) in companies and other corporate business arrangements. This article provides a doctrinal critique of the data protection mechanisms in Nigeria's Persons with Significant Control Regulations 2022 and the United Kingdom's PSC Regulations, as revised by the Economic Crimes and Corporate Transparency Act 2023. The article draws from data protection scholarship, constitutional law, and the Nigeria Data Protection Commission's (NDPC) published guidance. It identifies three design flaws in the data protection mechanisms in Nigeria's PSC Regulations: First, there is an undefined disclosure authority. Secondly, there is the absence of a proportionality assessment, and thirdly, there is the absence of a mechanism for guaranteeing the actual identity of PSCs. The UK's PSC Regulations demonstrate the constitutional ability of a public register framework to protect private interests. The article combines an unprecedented systematic comparison of the constitutional and data protection frameworks regarding Nigeria's PSC Regulations with legal scholarship and provides five specific recommendations for legislative reforms.

Keywords: Public register, private rights, persons with significant control, beneficial ownership, data protection, proportionality

Introduction

The Paradox of the Transparent Public Register

At its most elementary level, the implementation of a public register for beneficial ownership in companies and other corporate business arrangements represents the decision of Governments to demand that private individuals place their personal information within the universal gaze of scrutiny for the sake of the collective good: to support the fight against money laundering, to unveil illicit financial flows, and to curtail corporate criminality. The imperative for beneficial ownership transparency has received broad acceptance among scholars as a critical mechanism for deconstructing the opaque corporate arrangements that enable kleptocracy, corruption, and tax evasion [1]. Transparency, no matter how well-intentioned, hurts the individuals subjected to it. It is the exercise of the State's power that justifies the breach of the reasonable expectation of individuals that their personal information, including their identity, address, and financial information, will remain private and will not be made public without their consent. The breach of those expectations is only justified by the existence of a legislative framework that codifies the service to the public interest as a justification for the breach and provides mechanisms for the protection of individual rights.

The PSC Regulations under the Companies and Allied Matters Act 2020 (CAMA), alongside the Corporate Affairs Commission's Open Central Register of Beneficial Ownership (OCRBO), are a novel addition to Nigeria's regulatory landscape. They provide a mechanism to fulfill the promises made to participants at the 2016 London Anti-Corruption Summit and, to at least, nominally, align Nigeria with Recommendation 24 of the Financial Action Task Force [2]. However, unlike a number of other countries, the PSC Regulations were operationalised and implemented in Nigeria without the requisite constitutional and data protection frameworks, now established under Nigerian law. This article contends that the situation does not reflect a policy gap, but rather reveals a legal exposure that currently exists: the CAC is now operating a Public Register in a way that cannot be fully reconciled with the Constitution of the Federal Republic of Nigeria 1999 [3] (as amended) or with the Nigeria Data Protection Act 2023 (NDPA) and the regulatory and policy frameworks issued by the NDPC.

The United Kingdom as a jurisdiction, for example, provides a more effective legal framework for the PSC public disclosure obligation for companies and similar business arrangements. The public PSC register established in 2016 by the UK Companies Act 2006 has been iteratively built upon and refined further by the Economic Crime and Corporate Transparency Act 2023 (ECCTA), the UK General Data Protection Regulation (UK GDPR), and the Register of People with Significant Control (Amendment) Regulations 2025. The literature on the UK's PSC regime has advanced significantly [4]. However, the literature remains silent on a doctrinal comparative analysis of the data protection provisions in Nigeria's PSC regime vis-à-vis the UK's PSC regime as a constitutional issue and grounded in the NDPC's published guidance. This article seeks to remedy that omission.

The article is structured as follows. Part I introduces the discourse. Part II describes the relevant legal framework. Part III reviews the existing literature and identifies gaps as well as the importance of the research. Part IV explains the research findings and analysis in detail, and conducts a doctrinal audit of Nigeria's PSC Regulations, using NDPC's published guidance as the main source. Part V reviews the UK safeguards in multiple layers. Part VI engages in a

comparative discourse. Part VII puts forward five specific legislative recommendations while Part VIII wraps up the work.

Normative Framework- The Constitutional Right to Privacy and Data Protection Principles

1. Privacy as a Constitutional Right

The right to privacy is constitutionally, or at least, quasi-constitutionally guaranteed in Nigeria and the United Kingdom. Section 37 of the Constitution of the Federal Republic of Nigeria 1999 ('the Constitution') secures the privacy of Nigerian citizens from arbitrary acts of the State. As a fundamental right in Chapter IV of the Constitution, any limitation to this right must be provided for by the Constitution itself or some constitutional legislation, and must be reasonable and justifiable in a democratic society [5].

In the United Kingdom, Article 8 of the European Convention on Human Rights, as incorporated in the Human Rights Act 1998, protects the right to private and family life. Article 8 (2) of the Convention allows for the limitation to this right by the State only when such limitation is provided for by law, is aimed at a legitimate purpose, and is necessary in a democratic society [6]. Rivers shows that the proportionality principle, as set out in the Human Rights Act, obligates the Courts to ascertain whether a regulatory measure's limitation of a protected right is the least intrusive of the available options to achieve the measure's purpose [7]. This necessitates a bespoken and evidence-based approach to legislative design.

2. The NDPA 2023 and NDPC Implementation Guidance

The Nigerian data protection legal framework has transitioned from the Nigeria Data Protection Regulation 2019 (NDPR) to the NDPA 2023. The NDPA 2023 was signed into law on 12 June 2023, and establishes the Nigerian Data Protection Commission (NDPC) as an independent regulatory body. Babalola sees Nigeria's situation before the NDPA as one in which various legal frameworks were loosely established, and enforcement was weak [8]. The NDPA's principal legislative structure and the NDPC's exercise of enforcement power address this critique to a large extent.

The NDPC's General Application and Implementation Directive (GAID), NDPC/NDPA-GAID/001/2024, issued on 20 March 2025, is the first implementation guidance of NDPA 2023 and provides an application of the NDPA 2023 and Interpretative guidance. The GAID is significant to the analysis because it provides that the NDPA's constitutional obligations includes "all data processes and transactions in Nigeria," and therefore encompasses processes and transactions that take place in public institutions in Nigeria [9]. The NDPC's Public Sector Data Protection Compliance Circular further advances the NDPA's obligations by stating that all Ministries, Departments, and Agencies (MDAs) of the Federal Government of Nigeria are data controllers for the NDPA, Data Protection Impact Assessment, and Data Protection compliance and implementation [10].

Juma and Faturoti argue that while the data protection frameworks of Kenya and Nigeria are built on comprehensive legislation, implementation capability and enforcement remain the main issues [11]. The same applies to the NDPA 2023 and the PSC Register.

3. The UK GDPR and ICO Oversight

The UK General Data Protection Regulation (GDPR), which preserves the main framework of the EU's GDPR, applies to Companies House's processing of personal data. Article 35 of the UK GDPR requires a Data Protection Impact Assessment (DPIA) to be conducted where a processing activity is likely to pose a high risk to the rights and freedoms of data subjects, and the Information Commissioner's Office (ICO) is obligated to enforce the provision [12].

4. The Proportionality Principle in Register Design

The most prominent interpretation of the principle of proportionality in the design of beneficial ownership registers for companies and similar business arrangements was provided by the Court of Justice of the case of European Union in WM and Sovim SA v Luxembourg Business Registers (Joined Cases C-37/20 and C-601/20, 22 November 2022). In that case, the Grand Chamber of the EU Court of Justice struck down the Fifth Anti-Money Laundering Directive's provision mandating unrestricted public access to beneficial ownership registers, holding that such a requirement would constitute a serious and disproportionate infringement of the rights to privacy and the protection of personal data. Although the ruling is not binding on Nigeria or the post-Brexit UK, it is the most important case regarding the balance between privacy right and transparency obligations [13].

Open Ownership's foundational report asserts that public beneficial ownership registers for companies and similar business arrangements may satisfy the principle of proportionality, provided that appropriate safeguards and limitations are observed and embedded in the access and disclosure framework [14]. This is the standard that Nigeria's extant PSC Regulations do not meet.

Review of Literature, Knowledge Gaps and the Study's Importance

1. Current Research on Beneficial Ownership Transparency

Knobel, Harari, and Meinzer provide the most extensive empirical work on beneficial ownership registration by surveying 133 jurisdictions and demonstrating the range of varying disclosure thresholds, verification, and public access [15]. Martinez's review assesses the progress and challenges of global beneficial ownership transparency. Heathershaw and Prelec analysed the demand for transparency in the context of corporations' sophisticated concealment and, in that context, examined networks that sustain kleptocracy [16]. Adeyeye presents an account of the UK PSC and high-profile corporate misconduct [17], and Sharman's work on shell companies presents the political-economy context in which legislative decisions in both jurisdictions are situated [18]. The Tax Justice Network (TJN) 2024 reported on "privacy washing" and argues that privacy claims may be used to resist legitimate transparency demands. This article addresses the concern that argues that privacy claims may be used to resist legitimate transparency demands while drawing the line between corporate opacity and the constitutional rights of individual PSCs [19].

2. Current Research on Nigeria's PSC and Data Protection Frameworks

In respect of the PSC Regulations 2022, Nigerian legal scholarship is in its early stages. The most-cited

practitioner-oriented accounts are UUBO's 2023 client update and Afriwise's analysis. Both works highlight the undefined "Competent Authority" as a concern and fail to provide a systematic rights-based audit [20]. Regarding Nigeria's data protection framework, Babalola's 2022 article on International Data Privacy Law provides a survey of Nigeria's legal and institutional framework [21]. His 2024 article identifies the institutional tensions with the NDPA 2023, which is a legal transplant of the GDPR [22]. Singler and Babalola situate tensions within the North-South dynamics of diffused privacy rights [23]. There is also more commentary on NDPA 2023 in the UCC Law Journal and in the NDPC's own journal [24]. A comparative study of Juma and Faturoti warns of gaps in institutional capacity to translate these laws into regulatory practice [25].

3. Gap in Knowledge on Public Registers and Privacy Rights

The review of existing scholarship reveals a significant knowledge gap on public register for PSC in companies and similar business arrangements and privacy rights. There is a growing literature on beneficial ownership transparency, the PSC of Nigeria, and Nigeria's data protection framework, with a remarkably low interaction among the three. So far, no research has been published that: (i) carried out a constitutional audit of Nigeria's PSC regulations vis-a-vis section 37 of the Constitution and the NDPA 2023, as a combined effort; (ii) offered a sustained doctrinal analysis of the Nigeria's PSC vis-a-vis the data protection framework of the UK, the ECCTA 2023 and the 2025 Amendment Regulations, and the comparative context; (iii) recognised the legislative design failures outlined in this article as legal flaws that warrant specific legislative interventions; and (iv) used the NDPC's released guidance instruments as principal sources to analyse the CAC's compliance obligations regarding the PSC Register [26].

This research offers significant interventions. First, the work offers a systematic constitutional audit of Nigeria's PSC Regulations 2022 alongside the NDPC's primary implementation instruments, and an accompanying systematic data protection audit. Two, it seeks to aid comparative legal research by positioning Nigeria's data protection framework through systemic comparison with the UK's, which is the most closely linked data protection framework to Nigeria's history and being the country with the most evolved PSC regime. Third, the work advances the NDPA 2023 scholarship by demonstrating that the legislation uses cases and the operational government data services within a contextual and regulatory framework. Lastly, the work puts forward five reform initiatives in Part VII, which are designed to be immediate, feasible, and comparative, while remaining within the bounds of Nigeria's institutional realities.

Nigeria's Psc Regulations 2022- A Doctrinal Critique

1. Legislative Framework and Scope of Nigeria's PSC Regulations 2022

Nigeria's Persons with Significant Control (PSC) Regulations 2022 were made pursuant to section 867 of CAMA 2020, which apply to businesses incorporated under Part B (LLPs); under Part C (foreign exempted companies and LLPs and companies wholly owned by the Government). A PSC is any person who, either in their own right or through a trust or a partnership, holds at least 5% of the shares or voting rights of a company or who has the right to appoint or remove the majority of the directors or partners of a company, exercises control or significant influence of a company, and who meets the conditions specified above [27]. Nigeria's PSC Regulations 2022 set a 5% PSC threshold, which is considerably lower than the UK Regulations' 25% threshold.

Knobel, Harari, and Meinzer contend that while lower PSC thresholds may be good for capturing concealed control in companies and other business arrangements, they also expose far more people [28]. In Nigeria, the situation is even more troubling, as the stakes for data protection rise with additional design failures.

2. First Design Failure: The Undefined "Competent Authority"

The PSC Regulations 2022 allow disclosure of PSC information to law enforcement agencies, investigation agencies and any other relevant "Competent Authority." The PSC Regulations do not however define what is meant by "Competent Authority [29]." There is no definition for "Competent Authority" in CAMA 2020, nor in any of the other related Regulations. This omission is a significant and serious defect of statutory and constitutional dimensions. The NDPA 2023 provides that a lawful basis for the processing of personal data must be clearly established, and the NDPC's GAID specifies that the lawful basis must be identified before the processing of personal data and the same may not be changed after the fact [30]. The disclosure to an undefined category of recipients would not satisfy this requirement**.** Babalola demonstrates that the NDPA's GDPR-derived architecture demands "purpose specification" — the obligation to identify in advance, the precise purposes for processing personal data and the specific categories of the recipients [31].

The NDPC's Public Sector Data Protection Compliance Circular mandates all federal agencies to "identify and document a clear and specific lawful basis for each category of personal data processed" and "ensure that the disclosure of personal data to third parties is supported by a distinct lawful basis identified in advance [32]." Disclosure to an unspecified category of "competent authorities" does not meet the requisite standards. It also undermines the PSCs' NDPA 2023 rights of access and objection, as PSCs do not know to whom their personal data may be disclosed.

3. Second Design Flaw: No Proportionality Assessment and DPIA

The PSC Regulations do not provide for a proportionality assessment or Data Protection Impact Assessment (DPIA) prior to the public disclosure of PSC information. There is no evidence to suggest that a DPIA was conducted by any of the regulatory agencies prior to the launch of the Open Central Register in May 2023 or after the enactment of the NDPA 2023 [33]. The NDPA 2023 is clear in its provisions. The NDPA 2023 stipulates that a data protection impact assessment is a prerequisite to any processing of personal data "likely to result in a high risk to the rights and freedoms of data subjects [34]." DPIAs are required by the NDPC's GAID for any processing of personal data that involves "large-scale processing of personal data," "systematic monitoring of," or data that "significantly affects" data subjects, and includes public registers [35].

As part of Open Ownership's guidance, governments that implement public registers are suggested to do systematic proportionality assessments, which would include identifying public data categories, identifying what purposes are served by public versus restricted access, and what risk mitigation measures are in place for individuals who would be described as being at a greater risk [36]. The NDPC's Guidelines for the Management of Personal Data by Public Institutions state that public institutions are obliged to assess the necessity and proportionality of each data category to be processed and disclosed [37]. There is no evidence that Nigeria's PSC Register has considered any of the above elements.

4. Lack of Identity Verification Systems as a Design Flaw

The Corporate Affairs Commission (CAC) regulation enables participants to submit their PSC information directly to the CAC. Without verification against an official record, self-declaration is the only means of ensuring accuracy. The NDPC's Guidance Notice Registration of Data Controllers and Data Processors of Major Importance states that a data controller of major importance includes any organisation that processes the personal data of more than 200 data subjects within six months. The CAC's PSC Register far exceeds that threshold. Therefore, the CAC is required to fulfill all the responsibilities of a major data controller under the NDPA 2023 [38]. Among these responsibilities is the accuracy principle, which requires the CAC to ensure that the personal data in the Register is accurate and kept up to date. Without identity verification, it is systemically impossible for the CAC to fulfill that responsibility, as there is no mechanism to ensure that the self-declared information is correct. This is further supported by Knobel and Meinzer, who argue that an effective system of beneficial ownership registration requires verification [39]. Furthermore, self-declaration without verification produces poor-quality data that will not achieve its intended purpose in the fight against money laundering [40].

UK's PSC Framework- A System of Carefully Calculated Trade-Offs

1. Legislative Foundation: Companies Act 2006

The framework for the UK's PSC system was established under the Small Business, Enterprise and Employment Act 2015, which amended the Companies Act 2006, and was implemented in April 2016 [41]. From the outset, the system established two baseline data minimisation safeguards. The first is that PSCs' residential addresses are not made public; instead, service addresses are provided. The second is that complete dates of birth are not made public [42]. The foregoing matters reflect a deliberate legislative foundation that the transparency objective does not require the most sensitive personal data to be universally accessible. The evolution of the regime has been shaped by successive high-profile corporate misconduct disclosures — the Panama Papers, FinCEN Files, and the Pandora Papers — that demonstrated both the value of transparency and the inadequacy of unverified, self-declaratory registers [43].

2. The UK GDPR and ICO Oversight

The UK Companies House operates as a data control system that is subject to the UK GDPR and the Data Protection Act 2018, with the ICO as an independent supervisory authority. Within this framework, several externally enforceable obligations are vested — lawful bases, published privacy notices, DPIAs for high-risk data processing, data subject rights, and accountability. The ICO has a proven enforcement track-record against public sector bodies, which ensures a measure of accountability in the system [44].

3. The Economic Crime and Corporate Transparency Act (ECCTA) 2023: Four Key Innovations

3.1 Mandatory Identity Verification

ECCTA 2023 has made it mandatory for the personal identities of all PSCs to be verified either through GOV.UK One Login or an Authorised Corporate Service Provider, with the legal requirement coming into force on 18 November 2025. Identity Verification has both accuracy and deterrent functions. It provides the means to track PSCs and makes the PSC record a legally verified document [45].

3.2 Formal Suppression and Protection Mechanism

Under ECCTA 2023 and the Register of People with Significant Control (Amendment) Regulations 2025, PSCs with a credible threat or risk of personal injury or harm can request the UK Companies House to have their personal data suppressed. Applicants for data suppression must provide supporting evidence and the Registrar is empowered to reject applications without supporting evidence. Under that regime, information that is made unavailable to the public remains accessible to law enforcement agencies and other designated authorities [46].

3.3 Active Gate-keeping and Civil Financial Penalties

Under the ECCTA, the Companies House is no longer a passive filing repository but is authorised to function as an active gatekeeper and may query, challenge, and refuse to accept information for the register. Civil financial penalties for non-compliance are more flexible enforcement tools than criminal prosecution, introduced by the Economic Crime and Corporate Transparency Act 2023 (Financial Penalty) Regulations 2024 [47].

3.4 Law Enforcement and Tiered Access Data-Sharing

The UK establishes a four-tiered approach to data access: information that is publicly available; information available to obliged entities for AML due diligence; information available to credit referencing agencies under specified conditions; and information available to law enforcement and other specified authorities via formal request [48]. The ECCTA further authorises the Companies House to share protected information with law enforcement agencies when necessary and justifiable. This tiered access model exemplifies the principle of proportionality [49].

Comparative Analysis of Nigeria and the UK Regime

1. Disclosed Data Thresholds, Scope and Volume

An important structural difference between Nigeria and the UK systems is the PSC threshold: 5% in Nigeria and 25% in the UK [50]. The data protection implications are significant. Reducing the disclosure threshold encompasses a broader group of stakeholders. This group comprises individuals who may hold minority ownership positions in companies and regulated business arrangements and have different personal risk profiles from major stakeholders. However, there are no protections for members of this group as described in Part IV. The UK's higher threshold

incorporates a data minimisation function that is absent in Nigeria's regime.

2. Definition of a Competent Authority and Access to Structured Data

The greatest divergence between Nigeria and the UK frameworks concerns who can access non-public PSC information. The UK's framework grants a right to access private PSC information to a closed list of authorities. These include credit reference agencies, certain public authorities, and the Police; each of which is afforded access in accordance with the provisions of the Companies Act 2006, the UK GDPR, and the Data Protection Act 2018. Such a framework enables PSCs to understand who can access their information, and under what circumstances, and provides the Courts with a basis for reviewing access decisions.

Nigeria's PSC Regulations completely leave the term "Competent Authority" undefined. The NDPA 2023 and the NDPC's GAID assert that the lawful basis for disclosure and the identification of specific recipient categories must be determined before the processing of data. The PSC Regulations do not fulfill either of the above provisions [51]. The NDPC's Public Sector Data Protection Compliance Circular further directs federal agencies to maintain records of all third-party data disclosures, including the specific legal justification for each. Without a clearly defined category of authorised recipients, this obligation becomes impossible to satisfy [52].

3. Data Protection Oversight and Institutional Framework

In the UK, the Companies House can be scrutinised independently by the ICO, which has the power to impose financial penalties on public sector bodies, and has a record of exercising its supervisory powers [53]. The NDPC, established by the NDPA 2023, which has already imposed significant fines on private-sector companies [54], has thus far refrained from scrutinising CAC's PSC Register in a data protection oversight context [55]. Juma and Faturoti's assertion that the enforcement and institutional capacity of data protection law are of primary importance applies in this case: [56] the NDPC's PSC Data Protection Compliance Circular has already instructed federal agencies to appoint a Data Protection Officer (DPO) and to establish formal procedures for data subject requests. The CAC has not publicly demonstrated that it has satisfied these requirements regarding the PSC Register.

4. Rights-Compatible Legislative Process

Each of the UK's successive reforms contain rights-compatible provisions [57]. The PSC regime has been accompanied by consultation, parliamentary oversight, an impact assessment, and a section 19 Human Rights Act 1998 statement of compatibility [58]. That is an example of a legislative philosophy that recognises that regulatory frameworks for beneficial ownership transparency have costs and benefits implications and require the balancing of the rights that will be affected. Nigeria's PSC Regulations were issued as a single subordinate legislative instrument, with no prior rights-impact assessment, no consultation, and no framework for assessing compliance with the Regulations.

The NDPC's GAID creates requirements after the register's launch that the Regulations did not anticipate. Singler and Babalola argue that this phenomenon is a persistent aspect of externally influenced legal transplants in Nigeria, characterised by the Nigerian legal framework's formal compliance with global standards, undertaken without its actual operationalisation to guarantee the protection of substantive rights [59].

5. Identity Verification and Register Integrity

The UK's system of mandatory identity verification, which became effective in November 2025, is a positive response to a risk that, in many cases, has eroded the value of public beneficial ownership registers: self-declaratory registers often include either false identities or identities that have been improperly obtained, which exposes innocent people to the risk of self-disclosure and decreases the registers' transparency. Verification of identities in public registers strengthens the register's utility from an anti-money-laundering (AML) perspective and reduces the register's risk in the context of data protection.

As currently designed, Nigeria's self-declaration register is deficient in both areas. The NDPC's GAID requires data controllers to implement certain measures to ensure data accuracy. This requirement is impossible to meet without the infrastructure to support verification [60]. Therefore, the CAC's current approach fails both the NDPA 2023's accuracy requirement and the transparency objective that it is intended to serve.

Reform Proposals

1. Definition of the "Competent Authority" by Legislation

In order to comply with the PSC Regulations, the NDPA 2023 as the Nigerian legal framework, the NDPA should define what is meant by "Competent Authorities" as used in the NDPA 2023, for obtaining non-public PSC information, thereby creating a clear legal basis for such information to be obtained. This will satisfy the NDPA 2023's accuracy and transparency requirements and operationalise the FATF's notion of "Competent Authority" in the context of information that is not publicly available [61].

2. Commission and Publish a Retrospective DPIA

The NDPC and the CAC are challenged to jointly commission and publish a Data Protection Impact Assessment (DPIA) of the PSC Register. Obligations relating to high-risk data processing of the PSC Public Sector Data Protection Compliance Circular and NDPA 2023 are applicable in this context [62]. Given the high risk of targeted harm from data containing unique identifiers, the CAC should consider restricting access to such identifiers in the interim, until appropriate measures are enshrined.

3. Enactment of Statutory Tiered Access Framework

Nigeria should move away from a binary disclosure framework and establish a statutory tiered-access framework which should be enforced through the primary or subordinate legislation under CAMA 2020 and implemented using role-based access controls on the CAC digital interface. The NDPA 2023 embraces the principle of data minimisation and, as outlined in the NDPC's GAID, elaborates that data which is made available should be limited to what is necessary to achieve a specific purpose. The current unrestricted PSC public access framework fails to satisfy this principle, whereas a properly constructed tiered-access framework would do [63].

4. Mandatory Identity Verification

The PSC Regulations should be amended to require identity verification as a prerequisite for valid PSC registration. This may be accomplished using the NIMC database, BVN, or certified corporate service providers. Current PSC registrations should undergo verification processes, with emphasis on sectors at higher risk. In that regard, all unverified entries should be marked. Such change should help to meet the requirement in the NDPA 2023 concerning accuracy and the NDPC Guidance Notice, which stipulates that the CAC, as a primary data controller, must keep the processed personal data trustworthy.

5. Formalisation of the NDPC-CAC Regulatory Relationship

The Nigeria Data Protection Act (NDPA) 2023 demands a deeper, systemic integration across federal agencies. Specifically, Section 5(h) of the Act mandates that the Nigeria Data Protection Commission (NDPC) should co-operate with domestic authorities to achieve its regulatory objectives. The NDPC and CAC should sign a formal co-operation Memorandum of Understanding (MOU) in line with Section 5 (h) of the NDPA.

The MOU should offer a description of the responsibilities regarding the PSC Register, provide a joint DPIA and audit framework, specify obligations flowing from the CAC to notify data breaches to the NDPC within 72 hours stipulated by the NDPA 2023 and provide for data subject access request mechanism for PSCs. The MOU should also obligate CAC to publish a privacy notice for the PSC Register that complies with the NDPA.

Conclusion

Public registers and private rights are not enemies. They become enemies only when legislation fails to construct the architecture that reconciles them. This article reveals, through a doctrinal analysis set in comparative constitutional law, data protection principles, and the NDPC's guidance instruments, that Nigeria's PSC Regulations 2022 exhibit three identifiable legislative design failures. The failures consist of lack of definition of the "Competent Authority" in the NDPA 2023, the absence of DPIA and proportionality assessment; and the absence of identity verification and protection tools. The above are not abstract policy failures. They are established legal failures in a public system that currently operates in violation of the NDPA 2023 and the NDPC's guidance.

Almost a decade of legislative iteration has refined the UK's PSC system. Its design illustrates that coherence in constitutional design is not in conflict with successful anti-money laundering systems. The ECCTA 2023, the UK GDPR, the Data Protection Act 2018, and the 2025 Amendment Regulations collectively establish a legislative scheme that protects data subjects' rights while providing a responsive and proportionate system to their needs.

Existing within the Nigerian legal framework are the NDPA 2023, the NDPC's GAID, the Public Sector Data Protection Compliance Circular, and the Guidelines for the Management of Personal Data by Public Institutions. These legislative instruments provide a clear and unambiguous legal framework for reforming the PSC Register. The five proposals in Part VII of this work are not additional regulatory burdens on the CAC but rather minimal requirements for compliance with extant Nigerian laws.

Transparency should be sustained within the context of the rule of law, which entails the protection of the individuals and requires the justification, precision, and necessary safeguards that both the Constitution and the NDPA 2023 provide.

References

1. Antonio Lopo Martinez, 'Beneficial Ownership Transparency: Accomplishment and Obstacles' (2021) SSRN 3820479.
2. Corporate Affairs Commission (Nigeria), 'Beneficial Ownership Register: What You Need to Know' (May 2023) <ndpc.gov.ng> accessed 1 May 2026; UUBO, 'Client Update — Persons with Significant Control Regulations 2022' (March 2023) <uubo.org> accessed 1 May 2026.
3. CFRN 1999, s 37.
4. Adeyeye, 'Are Beneficial Ownership Laws Important? Exploring the Impact of Panama, FinCEN, and Pandora Papers on Beneficial Ownership Laws in the UK and the US' (2024) ScienceDirect; UUBO (n 2).
5. Constitution of the Federal Republic of Nigeria 1999 (as amended) s 37; Olumide Babalola, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12 International Data Privacy Law 44, 45.
6. Human Rights Act 1998 s 1 and Sch 1, art 8; European Convention on Human Rights (1950) art 8(2).
7. Julian Rivers, Proportionality and Deference under the UK Human Rights Act (CUP 2007); R v Secretary of State for the Home Department, ex parte Daly [2001] UKHL 26, [27] (Lord Steyn).
8. Olumide Babalola, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12 International Data Privacy Law 44, 46–49; Olumide Babalola, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant' (2024) 3 British Journal of Cyber Criminology 1.[1]
9. [Nigeria] Data Protection Commission (NDPC), General Application and Implementation Directive (GAID) NDPC/NDPA-GAID/001/2024 (20 March 2025), para 3.1 <ndpc.gov.ng>, accessed 1 May 2026. The GAID clarifies that the NDPA's constitutional obligation extends to "all data processes and transactions in Nigeria," expressly including those of public institutions.
10. NDPC, Public Sector Data Protection Compliance Circular (2023) <ndpc.gov.ng> accessed 1 May 2026. The Circular makes clear that all ministries, departments, and agencies of the Federal Government are data controllers subject to the full obligations of the NDPA 2023, including the requirements of lawful basis, DPIA, and data minimization.
11. Ifeoluwa Juma and Bola Faturoti, 'Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice' (2025) Computer Law & Security Review (University of Hertfordshire Research Archive) 15.
12. UK General Data Protection Regulation, art 35; Information Commissioner's Office, 'Conducting Privacy Impact Assessments Code of Practice' (updated 2024) <ico.org.uk> accessed 1 May 2026.
13. WM and Sovim SA v Luxembourg Business Registers (Joined Cases C-37/20 and C-601/20) EU:C:2022:912

(CJEU, Grand Chamber, 22 November 2022) paras 61–77.

14. Adriana Edmeades-Jones, Tom Parker and Tom Walker, Data Protection and Privacy in Beneficial Ownership Disclosure (Open Ownership, The B Team and The Engine Room 2019) <openownership.org> accessed 1 May 2026, 12–18
15. Andres Knobel, Markus Harari and Markus Meinzer, 'The State of Play of Beneficial Ownership Registration: A Visual Overview' (2018) Tax Justice Network; Andres Knobel and Markus Meinzer, 'State of Play of Beneficial Ownership — Update 2020' (2020) SSRN Electronic Journal.
16. Heathershaw and Prelec (n 1); John Heathershaw and others, The UK's Kleptocracy Problem (Chatham House 2021).
17. Adeyeye (n 3) 4–7; Tax Justice Network, Privacy Washing and Beneficial Ownership Transparency: Dismantling the Weaponisation of Privacy Against Beneficial Ownership Transparency (March 2024) <taxjustice.net> accessed 1 May 2026.
18. Jason C Sharman, The Despot's Guide to Wealth Management (Cornell University Press 2017) chs 3–4.
19. Tax Justice Network (n 17) 1–5.
20. UUBO (n 2); Afriwise, 'The Beneficial Ownership Register: Implementing the FATF's Recommendations on Money Laundering and Terrorism Financing in Nigeria' <afriwise.com> accessed 1 May 2026.
21. Babalola, 'Nigeria's Data Protection Legal and Institutional Model' (n 7) 44–52.
22. Babalola, 'GDPR-Styled NDPA 2023' (n 7) 5–8.
23. Samuel Singler and Olumide Babalola, 'Digital Colonialism Beyond Surveillance Capitalism? Coloniality of Knowledge in Nigeria's Emerging Privacy Rights Legislation and Border Surveillance Practices' (2024) 38(5) Information, Communication & Society.
24. A Critical Analysis of the Nigeria Data Protection Act 2023: Elevating Standards to Global Norms' (2025) UCC Law Journal; NDPC, 'NDPC International Journal of Data Privacy and Protection' (2024) vol 1 <ndpc.gov.ng> accessed 1 May 2026.
25. Ibid n10
26. As of January 2024, sixty-five per cent of African Union member states had enacted comprehensive data protection legislation: Juma and Faturoti (n 10) 3.
27. Persons with Significant Control Regulations 2022 (Nigeria) reg 14.
28. Knobel, Harari and Meinzer (n 14) 8–12.
29. Persons with Significant Control Regulations 2022 (Nigeria) reg 9(2)(c).
30. NDPA 2023 s 25; NDPC, General Application and Implementation Directive (GAID) NDPC/NDPA-GAID/001/2024 (20 March 2025) para 4.2 <ndpc.gov.ng> accessed 1 May 2026. The GAID expressly provides that the lawful basis for data processing "must be identified prior to the processing taking place" and that the basis cannot be changed retrospectively.
31. Babalola, 'GDPR-Styled NDPA 2023' (n 7) 5–7; NDPA 2023 s 24(1)(b) (purpose limitation) and s 25 (lawful basis requirement).
32. NDPC, Public Sector Data Protection Compliance Circular (2023) s 3 <ndpc.gov.ng> accessed 1 May 2026. The Circular specifically directs all federal government bodies to "identify and document a clear and specific lawful basis for each category ofpersonal data processed" and to "ensure that disclosure of personal data to third parties is supported by a distinct lawful basis identified in advance."
33. Corporate Affairs Commission (Nigeria) (n 2).
34. NDPA 2023 ss 24, 27, 28. Section 28 provides: "A data controller shall, prior to carrying out any processing which is likely to result in a high risk to the rights and freedoms of data subjects, carry out a data protection impact assessment."
35. NDPC, GAID (n 30) para 7.1–7.4. The GAID mandates that a DPIA must be conducted where processing involves "large-scale processing of personal data," "systematic monitoring," or data that "significantly affects" data subjects, and expressly includes public registers within the scope of this obligation.
36. Edmeades-Jones, Parker and Walker (n 13) 14–16.
37. NDPC, Guidelines for the Management of Personal Data by Public Institutions in Nigeria (2020) s 5 <ndpc.gov.ng> accessed 1 May 2026. Though issued under the NDPR, these Guidelines continue to apply as a baseline of public sector data governance. They require public institutions to "adopt a privacy-by-design approach to all data processing activities" and to "assess and document the necessity and proportionality of each category of data processed and disclosed."
38. NDPA 2023 s 24(1)(e) (accuracy principle); NDPC, Guidance Notice on Registration of Data Controllers and Data Processors of Major Importance (14 February 2024, updated in GAID 20 March 2025) s 3 <ndpc.gov.ng> accessed 1 May 2026. The Guidance Notice defines a data controller of major importance to include any entity processing the personal data of more than 200 data subjects in a six-month period — a threshold the CAC's PSC Register exceeds by orders of magnitude. The CAC is accordingly subject to the full obligations of a data controller of major importance under the NDPA 2023.
39. Knobel and Meinzer (n 14) 8.
40. Knobel and Meinzer (n 14) 8.
41. Small Business, Enterprise and Employment Act 2015 ss 81–111; Companies Act 2006 ss 790A–790ZG
42. Companies Act 2006 s 790LB (service address); s 790LF (date of birth).
43. Adeyeye (n 3) 4–7.
44. UK General Data Protection Regulation arts 5, 13, 35; Data Protection Act 2018 s 2; Information Commissioner's Office, 'Regulatory Action Policy' (2023) <ico.org.uk> accessed 1 May 2026.
45. Economic Crime and Corporate Transparency Act 2023 s 13; Registrar (Identity Verification and Authorised Corporate Service Providers) Regulations 2025; A&O Shearman, 'Economic Crime and Corporate Transparency Act 2023: Where Are We and What's Next?' (April 2025) <aoshearman.com> accessed 1 May 2026.
46. Register of People with Significant Control (Amendment) Regulations 2025; Companies House, 'Protecting Your Personal Information on the Companies House Register' (January 2023) <companieshouse.blog.gov.uk> accessed 1 May 2026.

47. Economic Crime and Corporate Transparency Act 2023 (Financial Penalty) Regulations 2024; Herbert Smith Freehills Kramer, 'Economic Crime and Corporate Transparency Act 2023: Implementing Radical Reforms to Companies House' (January 2026) <hsfkramer.com> accessed 1 May 2026.
48. Companies Act 2006 s 790LH; Companies House, 'Your Personal Information on the Public Record at Companies House' (updated November 2025) <gov.uk> accessed 1 May 2026.
49. Edmeades-Jones, Parker and Walker (n 13) 8–11.
50. Companies Act 2006 s 790C(2) (UK: more than 25%); Persons with Significant Control Regulations 2022 (Nigeria) reg 3 (Nigeria: at least 5%). See also Knobel, Harari and Meinzer (n 14) 9.
51. NDPA 2023 s 25; NDPC, GAID (n 30) para 4.2. See also Babalola, 'GDPR-Styled NDPA 2023' (n 7) 5–7.
52. NDPC, Public Sector Data Protection Compliance Circular (n 32) s 6. The Circular directs that federal agencies "shall designate a Data Protection Officer" and "shall establish a formal channel for receiving and responding to data subject access requests" — obligations that the CAC has not publicly demonstrated satisfying in relation to the PSC Register.
53. UK General Data Protection Regulation arts 5, 13, 35; Information Commissioner's Office (n 51).
54. For instance, ₦766.2 million fine imposed on Multichoice Nigeria and another fine of $220 million imposed on Meta Platforms.
55. NDPC enforcement record: NDPC imposed a ₦766.2 million fine against Multichoice Nigeria and a $220 million fine against Meta Platforms in 2024. See NDPC, Annual Performance Report 2023 (2024) <ndpc.gov.ng> accessed 1 May 2026; 'Nigeria Data Protection Law: Complete NDPA Compliance Guide 2025' <secureprivacy.ai> accessed 1 May 2026.
56. Juma and Faturoti (n 10) 15.
57. The iterative history of the UK regime spans: Small Business, Enterprise and Employment Act 2015; Information about People with Significant Control (Amendment) Regulations 2017; Economic Crime (Transparency and Enforcement) Act 2022; Economic Crime and Corporate Transparency Act 2023; Register of People with Significant Control (Amendment) Regulations 2025.
58. Human Rights Act 1998 s 19.
59. Singler and Babalola (n 23) 14; Babalola, 'GDPR-Styled NDPA 2023' (n 7) 8.
60. NDPC, GAID (n 30) para 7.3; NDPA 2023 s 28.
61. Financial Action Task Force, Guidance on Beneficial Ownership of Legal Persons (March 2023) para 4.3 <fatf-gafi.org> accessed 1 May 2026.
62. NDPC, GAID (n 30) para 7.1–7.4; NDPA 2023 s 28; NDPC, Public Sector Data Protection Compliance Circular (n 32) s 5. The Circular provides that federal institutions shall conduct a DPIA "before deploying any new data processing system or substantially modifying an existing system" — a requirement triggered, at a minimum, by the launch of the Open Central Register in May 2023.
63. NDPA 2023 s 24(1)(e); NDPC, Guidance Notice on Registration of DCPMIs (n 46) s 3.