Bridging the Divide: A Comparative Analysis of Data Subject Access Rights Under UK and Nigerian Data Protection Law

Ganiyat Omowunmi Issa[*]

Abstract

Subject access is a central data protection right because it enables individuals to know what personal data is held about them and how it is being processed. This article critically compares subject access rights under the United Kingdom General Data Protection Regulation and the Nigeria Data Protection Act 2023, with particular attention to the extent to which formal similarity produces effective protection in practice. Using a doctrinal and functional comparative approach, the article examines the substantive scope of the right, procedural requirements, costs, search obligations, competing interests, judicial interpretation and enforcement. The article finds substantial convergence between Article 15 UK GDPR and section 34 of the Nigeria Data Protection Act at the level of substantive entitlement. The more significant divide lies in operational certainty. While the UK regime has developed clearer standards through legislation, regulatory guidance and case law, important aspects of the Nigerian framework remain open to interpretation, particularly in relation to unreasonable delay, unreasonable costs, the extent of a controller's search obligation and the treatment of competing interests. The article further argues that Nigeria's challenge is not simply weak enforcement, since the Nigeria Data Protection Commission possesses significant statutory powers, but the limited development and visibility of subject-access-specific regulatory and judicial interpretation. The article concludes that bridging the divide requires domestic operationalisation rather than further wholesale transplantation of UK or GDPR rules. Clearer regulatory standards and greater publication of subject access decisions would strengthen the practical effectiveness of section 34 within Nigeria's own legal and institutional context.

Keywords: Controller; Data Protection, Legal Transplantation, Right of Access, Subject Access Rights ,

1 Introduction

The right of access occupies a central position in data protection law because individuals cannot meaningfully challenge the processing of their personal data if they do not know what information is held about them or how it is being used. Through a Subject Access Request (SAR), a data subject may obtain confirmation that personal data is being processed, access to that data and information concerning the circumstances of the processing. Access can therefore enable the exercise of related rights, including rectification, erasure and restriction, where the information obtained reveals inaccurate, unnecessary or otherwise questionable processing.[1]

---

[*] *LL.B (University of Ilorin), CIPP/E*

[1] Osigwe Billy Ademi and Kpea-Ue Bariyira Simple, 'Data Protection and the Rights of Workers in the European Union and the United Kingdom: Lessons for Nigeria' [2026] 21 *Journal of Jurisprudence, International Law and Contemporary Legal Issues* 234 <https://www.rsujilclijournal.com.ng/journal/index.php/jilcli/article/view/24> accessed 24 August 2026.

The United Kingdom and Nigeria both provide substantial statutory rights of access. Article 15 of the UK General Data Protection Regulation (UK GDPR)[2] gives a data subject the right to confirmation of processing, access to personal data and specified information concerning matters such as the purposes of processing, categories of data, recipients, retention and automated decision-making. Section 34[3] of the Nigeria Data Protection Act 2023 (NDP Act)[4] establishes a broadly comparable entitlement, including a right to a copy of the data subject's personal data. The apparent similarity between the provisions makes the two regimes suitable for comparison, but it also creates a risk of treating similarity in legislative language as evidence of equivalent protection.

That assumption is particularly important to interrogate in the Nigerian context. Nigeria's contemporary data protection framework has developed under considerable European influence. The Nigeria Data Protection Act as been characterised as a GDPR-influenced legal transplant and argues that the effectiveness of borrowed rules depends on their adaptation to Nigeria's legal, institutional and socio-economic conditions[5]. A few legal scholars[6] made a similar point in the wider African context, observing that EU-style legislation has frequently influenced African data protection laws while cautioning that the relevant question is whether transplanted rules can function effectively within the receiving legal environment. The significance of legal transplantation therefore extends beyond identifying similarities between statutes. It requires examination of whether the procedures and institutions necessary to make the transplanted right effective have also been developed.

Subject access provides a useful context in which to test this distinction. The statutory right may be broad, yet its practical value depends on questions that are not answered by the substantive entitlement alone. How easily can a request be made? How long may a controller take to respond? How much information may be required to verify identity? How extensively must the controller search for the requested data? Who bears the cost of a difficult request? When may access be restricted because of third-party interests or administrative burden? These questions determine whether the right can be exercised and enforced.

Recent developments make this comparison particularly timely. Nigeria's present statutory regime dates from the NDP Act 2023[7] and has subsequently been supplemented by the General Application and Implementation Directive 2025[8]. In the UK, the Data (Use and Access) Act 2025[9] has further developed the subject access framework, including by expressly providing that

---

[2] ibid 2

[3] Section 34 strips away the secrecy of data collection in Nigeria. It dictates that you must be told clearly and upfront why your data is being handled. It grants you the absolute right to view that data for free, force an organization to correct it if it contains errors, or order them to delete it entirely if they have no valid legal reason to keep holding onto it

[4] Nigeria Data Protection Act 2023.

[5] Olumide Babalola, 'The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplan' [2024] *Social Science Research Network* 3

[6] Patricia Boshe, Moritz Hennemann and Ricarda von Meding, 'African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward' [2022] 3 *Global Privacy Law Review* 56 .

[7] ibid 3

[8] Nigeria Data Protection Commission General Application and Implementation Directive 2025.

[9] Data (Use and Access) Act 2025.

controllers are required to conduct reasonable and proportionate searches when responding to access requests, thereby codifying a principle previously developed in domestic case law.

Existing scholarship provides a foundation for comparison but does not resolve this narrower question. Earlier[10] examinations of the statutory and regulatory frameworks for data protection in Nigeria and the United Kingdom existed, but these studies predate the NDP Act 2023 and therefore cannot assess the present Nigerian access regime. A more recent UK-Nigeria offers comparison, which ranges across the development, concepts and enforcement of data protection law rather than concentrating on subject access[11]. By contrast, a few focuses are primarily on the broader implications of GDPR-style legal transplantation[12], while others[13] address the development and transplantation of data protection regulation across Africa.

The problem addressed in this article is therefore not simply whether Nigerian law recognises a right of access comparable to that found in UK law. It is whether apparent substantive convergence is accompanied by sufficient procedural certainty, interpretative guidance and enforcement mechanisms to make that right effective. A comparison limited to Article 15 UK GDPR and section 34 NDP Act would not answer this question because the practical boundaries of access are also shaped by procedural rules, regulatory guidance, judicial interpretation and institutional enforcement.

1.1 Aim of the Article

The article critically compares subject access rights under UK and Nigerian data protection law to determine the extent to which formal similarity in the substantive right translates into comparable conditions for its exercise and enforcement. It also considers whether aspects of the UK experience provide useful lessons for Nigeria without treating the UK framework as a model that should be transplanted wholesale.

1.2 Research Question

The central research question is:

To what extent does Nigerian data protection law provide an effective right of access comparable to that available under UK data protection law?

The study further asks:

1. How do the substantive and procedural rules governing subject access rights in the United Kingdom and Nigeria converge and diverge?

2. How do controller obligations, limitations and enforcement mechanisms affect the practical effectiveness of subject access in both jurisdictions?

---

[10] Hafeez Folohunsho Zubair, '*Statutory and Regulatory Framework for Data Protection in Nigeria and United Kingdom'* [2021] SSRN <https://doi.org/10.2139/ssrn.3954296> accessed 24 August 2026.

[11] Kater Aorga, *'A Comparative Analysis of Data Protection Law Between Nigeria and the UK'* (SSRN 2025) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5206376> accessed 24 August 2026.

[12] ibid

[13] Ibid n8

3. What lessons can Nigeria draw from the UK experience in developing a subject access regime that is both effective and responsive to its own legal and institutional context?

1.3 Methodology and Scope of the Study

The article adopts a doctrinal and functional comparative legal approach. It analyses the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, the NDP Act 2023 and the General Application and Implementation Directive 2025 alongside relevant judicial decisions, ICO and NDPC materials and academic literature. The comparison is functional rather than merely textual: it examines how the two systems respond to common problems arising in the exercise of subject access, particularly accessibility, response time, identity verification, costs, search obligations, competing interests and enforcement. Other data subject rights and freedom of information law are considered only where necessary to explain the operation of subject access.

2 Analytical Framework: Subject Access and Legal Transplantation

2.1 From Formal Recognition to Effective Access

A comparison of Article 15 UK GDPR and section 34 of the NDP Act based only on their wording would reveal considerable similarity, but it would say little about whether the two rights are equally effective. The central issue is not simply what a data subject is formally entitled to receive, but what happens when that entitlement is exercised. A right of access becomes meaningful only where the requester can invoke it without unnecessary barriers, the controller can identify what compliance requires, and non-compliance can be effectively challenged.

This distinction shifts the comparison from formal equivalence to functional effectiveness. A broadly drafted access right may still operate unevenly where the law does not clearly determine matters such as the period for compliance, the permissible cost of access, the extent of the controller's search obligation or the circumstances in which competing interests justify withholding information[14]. Conversely, differences in statutory wording do not necessarily indicate weaker protection where regulatory or judicial interpretation supplies workable standards. The relevant measure is therefore the degree to which each legal system converts the statutory entitlement into a predictable and enforceable right.

This approach is particularly important because the existing Nigerian framework already contains substantial enforcement machinery. The question cannot therefore be reduced to whether Nigeria has enacted a right or created a regulator. The more difficult inquiry is whether the surrounding legal framework gives sufficient content to section 34 for data subjects and controllers to know, before a dispute arises, what effective compliance requires. This distinction between the law as enacted and the law as operationalised reflects a warning that the assessment of data protection regimes must account for their "living practice and enforcement", rather than legislation alone[15].

---

[14] Syahreza Fachran, Sinta Dewi Rosadi and Prita Amalia, ‘Protection of Data Subject Rights in the Transfer of Personal Data Between Data Controllers in Indonesia: A Comparative Analysis of the PDP Law and the EU GDPR’ [2026] 8 *Awang Long Law Review* 518 .

[15] ibid 6

2.2 Legal Transplantation and the Problem of Operational Fit

Legal transplantation is useful to this study not simply because the NDP Act resembles the GDPR, but because it raises a more difficult question about the operational fit of borrowed legal rights. It can be argued that the Nigerian data protection framework bears unmistakable similarities to the GDPR but cautions that transplantation without sufficient attention to Nigeria's cultural, socio-political and economic circumstances may create difficulties in implementation and enforcement. Similarly, question whether EU-inspired data protection rules can function effectively when transplanted into different legal and institutional settings have been raised.

This was[16] developed via a related argument through the concept of the "transplant effect". Drawing on comparative-law scholarship, scholars have argued that transplanted laws may function less effectively where the population and legal institutions are unfamiliar with them and where the rules have not been sufficiently adapted to local conditions. This consequently advocates the adaptation of data protection frameworks to domestic circumstances rather than the uncritical approximation of foreign standards.

For subject access, however, the significance of this critique lies less in the source of section 34 than in what the transplantation achieved. A legislature can reproduce the content of a right without simultaneously reproducing the interpretative and institutional framework through which that right becomes workable[17]. This distinction is evident in the UK, where the Article 15 entitlement operates alongside domestic legislation, regulatory guidance and judicial decisions that address questions left open by the statutory text. Nigeria's adoption of a comparable substantive entitlement does not automatically resolve those same questions.

The analytical issue is therefore whether section 34 has been sufficiently domesticated in operation. If the substantive entitlement is comparable but its boundaries remain uncertain when questions of delay, cost, search effort, competing rights or refusal arise, the weakness does not lie in the absence of a right. It lies in the gap between legislative borrowing and effective implementation. Babalola's[18] call for a Nigerian data protection framework capable of developing an identity beyond wholesale comparison with the GDPR is particularly relevant in this respect.

Accordingly, legal transplantation is used here as an explanatory rather than prescriptive framework. The UK is not treated as a model whose rules Nigeria must reproduce. Instead, the comparison tests whether similar access entitlements are supported by legal mechanisms capable of resolving the practical conflicts they generate. The question is ultimately not how closely section 34 resembles Article 15, but whether Nigerian law has developed the procedural, interpretative and institutional conditions necessary to make section 34 effective.

---

[16] Justin Bryant, *'Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and DigitalRights'*[2026]Heinonline.com<https://access.heinonline.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/stantlr24&section=9> accessed 24 August 2026.

[17] Cara Mannion, 'Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets' [2021] *Vanderbilt Law Review* 53

[18] ibid 4

3. Legal Framework for Subject Access Rights in the United Kingdom and Nigeria

The right of access in the United Kingdom and Nigeria is not contained in a single provision operating in isolation. In both jurisdictions, the substantive entitlement is supported by procedural rules, exemptions, regulatory guidance and enforcement mechanisms. Understanding the legal framework is therefore necessary before comparing how subject access requests are made and handled in practice.

3.1 Formal Convergence and the Limits of Textual Similarity

At first sight, Article 15 UK GDPR and section 34 of the NDP Act establish closely comparable rights. Both allow a data subject to obtain confirmation that personal data concerning them is being processed, access to that data and information concerning matters such as the purposes of processing, categories of data, recipients, retention and automated decision-making. Both also recognise a right to a copy of the personal data concerned. The Nigerian provision is therefore not a substantially weaker version of the UK right at the level of formal entitlement.

That convergence is important, but it has limited explanatory value. A comparison that ends with the similarity of Article 15 and section 34 risks treating the statutory statement of the right as synonymous with its effectiveness. Yet many of the questions that determine whether access is meaningful arise only after the right has been invoked. Neither an entitlement to a copy nor a right to processing information determines, by itself, how quickly the controller must respond, how extensively it must search, what burden may be transferred to the requester, or how conflicts with other rights should be resolved.

The comparison therefore reveals an important limit to substantive transplantation. Section 34 appears to have absorbed much of the content of the European-style access right, but the surrounding mechanisms through which that entitlement is translated into concrete controller obligations are not equally aligned. The significance of the UK framework lies less in Article 15 alone than in the way that Article 12[19], the Data Protection Act 2018, the Data (Use and Access) Act 2025, ICO guidance[20] and judicial interpretation collectively give Article 15 operational content. Current ICO guidance, for example, deals expressly with the form of a request, time limits, clarification, identification, fees and search obligations. The issue for Nigeria is therefore not whether section 34[21] recognises enough rights, but whether its broader legal framework defines those rights with sufficient certainty once compliance becomes contested.

3.2 Time, Formality and Identity: Accessibility versus Certainty

There is relatively little basis for identifying a serious divide in the formalities required to initiate access. In the UK, a SAR can be made verbally or in writing, including through social media,

---

[19] Data Protection Act 2018, s 12. The act makes provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes.

[20] Information Commisioner's Office (ICO), *General Data Protection* (Ico.org.uk, 29 August 2025) <https://ico.org.uk/about-the-ico/what-we-do/our-plans-for-new-and-updated-guidance/general-data-protection/> accessed 27 August 2026.

[21] NDP Act 2023 s.34

and does not depend on prescribed terminology or a mandatory form. Section 34 of the NDP Act similarly does not prescribe a particular form through which the right must be exercised. The NDPC's own SAR procedure expressly states that completion of its form is not compulsory, although the Commission considers that using it may facilitate processing.

The more significant issue arises once a request is received. Identity verification illustrates the tension between protecting personal data and avoiding unnecessary barriers to access. The UK position expressly requires a proportionate approach. The ICO advises that formal identification should only be sought where necessary and that controllers should not collect more information than is reasonably required to establish identity. This is not merely administrative advice. It allocates the risk between two competing harms: disclosure to the wrong person on the one hand, and obstruction of the data subject's right on the other[22].

Section 34 does not articulate an equivalent general proportionality test for identity verification. This creates a potential difficulty because an organisation could, in principle, protect itself against mistaken disclosure by demanding extensive identification from every requester. Such a practice might improve security but simultaneously require a person to surrender additional personal data to exercise a data protection right. The absence of a clear general standard therefore matters less because Nigeria lacks an identification mechanism than because the boundary between legitimate verification and obstructive verification remains less clearly defined.

The contrast is sharper in relation to time. UK law combines the obligation to act without undue delay with a definite one-month period, subject to specified extensions and, following the 2025 reforms, rules governing clarification and the pausing of time. Section 34 instead requires access without constraint or "unreasonable delay". The NDPC has adopted a 30-day target for requests made to the Commission itself, but that administrative practice is not equivalent to a generally applicable statutory deadline for all Nigerian controllers.

The weakness of the Nigerian formulation is therefore not that flexibility is inherently undesirable. A rigid period may itself be inappropriate for unusually complex requests. The difficulty is that "unreasonable delay" does not provide the same ex ante certainty. A data subject deciding whether to complain, and a controller deciding whether it is still within time, must first determine what reasonableness requires in the circumstances. The legal standard becomes clearest only after a dispute arises. In this respect, flexibility is obtained at the cost of predictability.

3.3 The Cost Barrier: Who Bears the Price of Access?

The treatment of cost reveals a more substantive difference in how the two regimes allocate the burden of compliance. Under the UK framework, access is ordinarily free. A controller may charge a reasonable administrative fee in limited circumstances, principally where a request is manifestly unfounded or excessive or where further copies are requested. The controller must also be capable of explaining and justifying the fee[23]. The default position therefore treats the

---

[22] Vanessa Villanueva Collao and Verity Winship, 'The New ICO Intermediaries' *[*2019] 5 *The Italian Law Journal* 5 <https://access.heinonline.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/italj5&section=39>.

[23] Sofia Roselin, Moody Rizqy and Syailendra Putra, 'Personal Data Subject Rights Protection: A Comparative Study Between Indonesian PDP Law and the UK Data Protection Act' [2025] 8 *Journal USM Law Review* 825.

cost of responding to a legitimate access request as part of the controller's compliance responsibility.

Section 34(1)(b) of the NDP Act adopts a different approach by permitting a data subject to bear some or all the cost where providing the personal data would impose "unreasonable costs" on the controller. The distinction is important because the Nigerian exception focuses on the cost to the controller, rather than necessarily on abusive conduct by the requester. A legitimate request may therefore attract a charge even though there is nothing excessive or improper about the individual's exercise of the right.

The provision raises questions that the statutory wording does not resolve. What expenditure qualifies as unreasonable? Is the controller permitted to include staff time, retrieval costs or the cost of reconstructing poorly managed records? Must the controller prove that the cost is exceptional rather than part of ordinary compliance? Most importantly, should deficiencies in an organisation's own record-management systems increase the price an individual must pay to exercise a statutory right?

These questions affect more than administrative convenience. Cost determines accessibility. An[24] analysis of access-to-information legislation, although concerned with freedom of information rather than subject access, makes the broader point that excessive access costs can discourage use of a legal right and disproportionately affect economically disadvantaged requesters. The same concern is relevant here by analogy. If "unreasonable costs" is capable of being interpreted broadly without defined safeguards, the practical value of section 34 may vary according to both the organisation's administrative efficiency and the requester's ability to pay.

The difficulty is therefore not that any form of cost recovery is necessarily illegitimate. Controllers should not be compelled to absorb limitless expense in every conceivable case. The problem is that section 34 shifts part of that burden to the data subject without itself supplying a sufficiently developed standard for determining when the shift is justified. That uncertainty risks turning a protective exception for controllers into a potential barrier to access.

3.4 Search Obligations: The Hidden Core of the Right

The obligation to search is perhaps the clearest example of why formal recognition cannot determine the effectiveness of subject access. A statutory right to obtain a copy of personal data has limited value if the law does not also establish how seriously the controller must attempt to locate that data.

UK law has developed a relatively clear answer. In *Dawson-Damer v Taylor Wessing LLP*[25], the Court of Appeal rejected the suggestion that a controller could rely on the scale or inconvenience of a search without demonstrating why further effort would be disproportionate. In *Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd*[26], the Court of Appeal treated the obligation as one of reasonable and proportionate search rather than an exhaustive duty to pursue every conceivable

---

[24] Omosede A Osawe, 'A Comparative Analysis of the Right of Access to Information Under the Nigerian Freedom of Information Act 2011 and the South African Promotion of Access to Information Act 2001' [2022] 22 *African Human Rights Law Journal* 1 <https://doi.org/10.17159/1996-2096/2022/v22n2a7>.

[25] *Dawson-Damer v Taylor Wessing LLP* [2017] EWCA Civ 74

[26] *Ittihadieh v 5-11 Cheyne Gardens RTM Co Ltd* [2017] EWCA Civ 121

source. The Data (Use and Access) Act 2025 has now placed that standard on an express statutory footing, and the ICO requires controllers to undertake a reasonable and proportionate search for responsive information.

The significance of this standard lies in the balance it creates. It protects the data subject from a superficial response while recognising that searching every archive, backup, device or historic record may sometimes impose a disproportionate burden. Crucially, proportionality is not a licence for non-search. It is a standard against which the adequacy of the controller's effort can be assessed.

Section 34 of the NDP Act necessarily presupposes retrieval because a controller cannot provide confirmation and a copy without locating the relevant data. Yet the provision does not expressly define the required intensity of that search. The GAID 2025 was issued partly to promote certainty in data protection obligations, but it does not establish a dedicated subject-access search standard comparable to the UK's reasonable and proportionate search rule.

This leaves a doctrinal gap at the point where the statutory entitlement is most dependent on controller conduct. An exhaustive search requirement could impose unrealistic burdens, particularly on controllers with extensive or fragmented records. At the other extreme, leaving search adequacy almost entirely to controller discretion risks hollowing out the right. A controller could technically recognise section 34 while undertaking only a minimal search and thereby determine, in practice, the amount of personal data the requester is able to obtain.

3.5 Competing Rights and Administrative Burden

Subject access also requires a legal framework capable of deciding when the individual's entitlement must yield to competing interests. This is particularly difficult where records contain third-party personal data, legally privileged communications or requests that impose exceptional administrative burdens[27].

UK law addresses these conflicts through a combination of Article 15(4), the Data Protection Act 2018 and regulatory guidance. The presence of third-party information does not automatically extinguish the requester's entitlement; the controller must consider whether disclosure can occur, including through redaction or a reasonableness assessment. Similarly, the framework provides defined exemptions for legally privileged material and permits manifestly unfounded or excessive requests to be refused or subjected to a reasonable administrative fee. The effect is not simply to restrict access, but to provide a structure for deciding when restriction is justified.

Nigeria faces the same conflicts but does not yet resolve all of them through an equally integrated subject-access doctrine. Section 34 provides a broad entitlement, while other Nigerian laws protect confidentiality and privilege and the NDP Act recognises the possibility of unreasonable costs. The difficulty is the relationship between these principles. The presence of a competing interest does not itself answer whether all information should be withheld, whether redaction is required, or whether only the affected part of the request may be restricted. This is particularly evident in relation to administrative burden. UK law distinguishes between the effort required to search, the excessiveness of a request and the circumstances in which a fee or refusal

---

[27] Sofia Roselin, Moody Rizqy and Syailendra Putra, 'Personal Data Subject Rights Protection: A Comparative Study Between Indonesian PDP Law and the UK Data Protection Act' [2025] 8 *Jurnal USM Law Review* 825.

is permissible. Nigerian law contains the "unreasonable costs" safeguard but does not articulate the same combination of search, burden and refusal standards. The result is not necessarily greater protection for either controllers or data subjects. Rather, it leaves the allocation of burden less coherent.

The operational divide identified in this section is therefore more precise than a general claim that UK law is detailed while Nigerian law is not. Section 34 establishes a substantial right, but several of the legal standards that determine who bears the risks and costs of exercising that right remain comparatively unsettled. The next issue is whether courts, regulators and enforcement institutions have been able to supply the missing operational content.

4. Interpretation, Enforcement and Institutional Effectiveness

The uncertainties identified above do not necessarily amount to permanent defects in the statutory framework. Open-textured legislation can acquire greater precision through judicial interpretation and regulatory practice. The more important question is therefore whether the institutions responsible for implementing subject access can convert broad statutory entitlements into predictable standards. On this issue, the comparison reveals a further divide: the UK right has developed through an interaction between legislation, adjudication and regulatory interpretation, whereas much of the operational meaning of section 34 remains to be developed.

4.1 Courts as Co-authors of the Right

The development of UK subject access law demonstrates that the practical content of the right cannot be attributed to Article 15 alone. Courts have played an important role in determining what compliance requires when the statutory entitlement encounters competing interests or administrative difficulty. Their significance lies less in the number of decided cases than in the legal standards those cases have produced.

UK case law established that controllers must conduct reasonable and proportionate searches, rather than exhaustive ones, when responding to subject access requests. It places the burden on controllers to justify claims of disproportionate effort[28], while also furthering the reinforcement of the proportionality standard. This judicial approach was later codified in the Data (Use and Access) Act 2025[29]. The same process can be seen in questions concerning the scope of disclosure. In *Ashley v Revenue and Customs*[30], the dispute was not simply whether the requester possessed a right of access, but how broadly personal data should be identified and how much surrounding context was necessary for the disclosed information to be intelligible. The importance of such litigation is that it moves the law from stating that access must be provided to determining what meaningful access requires. UK courts have therefore functioned, in practical terms, as co-authors of the access regime. Judicial interpretation has filled gaps between statutory language and organisational practice, while subsequent regulatory guidance and legislation have absorbed some of those principles. The evolution of the reasonable-search requirement is particularly illustrative: what began as a question of proportionality in litigation eventually became an express statutory rule.

---

[28] ibid 22

[29] ibid 23

[30] [2025] EWHC 134 (KB)

Nigeria has not yet developed a comparable body of reported jurisprudence specifically interpreting section 34. That should not be treated as evidence that the right itself is defective. The NDP Act has only been in force since 2023, and a younger statutory framework cannot reasonably be expected to possess the jurisprudential history of the UK regime. Nevertheless, the absence of subject-access-specific authority has present legal consequences. Questions already identified in this article, including what constitutes unreasonable delay, how unreasonable cost should be calculated and how extensive a controller's search must be, presently lack the kind of authoritative judicial clarification available in the UK.

The difficulty is therefore interpretative dependence. Section 34 creates the entitlement but leaves parts of its practical content dependent upon future decisions by the NDPC and the courts. The fact that this uncertainty may diminish as Nigerian jurisprudence develops does not remove its current effect on controllers and data subjects. A right whose boundaries become clear only after litigation places greater interpretative risk on those required to exercise or comply with it.

4.2 Enforcement Power versus Enforcement Effectiveness

The Nigerian regime should not, however, be characterised simply as institutionally weak. The NDP Act gives the NDPC substantial enforcement powers. Sections 46 to 48 permit investigation of alleged violations and the making of compliance and enforcement orders. Importantly, a compliance order may expressly require a controller or processor to comply with a data subject's request to exercise rights under the Act. Enforcement measures may also include remediation, compensation and financial sanctions, while section 51 provides a route to civil damages. These provisions complicate the proposition that the divide between the UK and Nigeria is one of regulatory power. At least formally, the NDPC has tools capable of compelling respect for section 34. The more difficult issue is whether exercise of those powers generates sufficient interpretative value beyond the individual case.

The distinction matters because enforcement performs two functions. The first is corrective: an individual whose request has been ignored or improperly refused needs an effective remedy. The second is norm-generating: the regulator's decisions tell other controllers what similar conduct will require in the future. It is the latter function that is particularly significant where legislation uses standards such as "unreasonable delay" or "unreasonable costs".

The NDPC's annual reports demonstrate increasing investigatory activity. Its 2024 report, for example, identifies investigations involving matters such as unauthorised access, loss of personal data and other infringements, while the 2025 report describes a continued expansion of enforcement and compliance activity. These materials establish that the Commission is active. They do not, however, provide sufficient subject-access-specific information to determine how frequently section 34 complaints arise, what standards the Commission applies to disputed SARs, or how questions such as cost, delay and search adequacy are resolved.

This produces a distinction between enforcement activity and enforcement visibility. A regulator may successfully resolve individual disputes without producing a body of publicly accessible reasoning capable of guiding the wider regulated community. Where decisions are not sufficiently published or disaggregated, controllers remain uncertain about the standard expected of them and data subjects have less material against which to assess whether a refusal or delay is contestable.

By contrast, the UK framework combines enforcement with extensive interpretative material. Current ICO guidance distinguishes between what organisations legally "must" do and what the regulator considers good practice and addresses the practical stages of handling access requests in detail. The comparative advantage is therefore not simply that the UK regulator has stronger powers. It is that regulatory interpretation has become part of the infrastructure through which the right acquires predictable meaning. For Nigeria, the analytical concern is consequently not an absence of enforcement machinery but the limited visibility of SAR-specific enforcement reasoning. In a developing regime, publication of anonymised decisions and complaint outcomes could partly perform the interpretative function that case law has played in the UK.

4.3 Independence, Transparency and Institutional Design

Regulatory effectiveness also depends on institutional independence, particularly where access is sought from public authorities. Section 1 of the NDP Act expressly envisages an impartial and independent Commission, and the NDPC has significant powers to investigate both public and private controllers. Yet the statutory design has attracted criticism. It could be argued that the Commission's independence is potentially weakened by executive involvement in its institutional structure, including the appointment of the National Commissioner on the Minister's recommendation and the Minister's power to issue general policy directives[31]. The Act confirms that the National Commissioner is appointed by the President on the Minister's recommendation, while section 60 permits ministerial directives of a general nature or relating to policy.

The significance of this criticism for subject access should not be overstated. Ministerial involvement does not, by itself, establish that the NDPC lacks operational independence or that individual enforcement decisions are politically controlled. Indeed, section 60 concerns directives of a general or policy nature rather than an express power to determine individual complaints. Treating institutional dependence as established merely from the existence of ministerial oversight would therefore go beyond what the statutory structure proves.

Nevertheless, the concern cannot be dismissed as irrelevant. A data protection regulator may be required to enforce access rights against ministries, departments and other public bodies. Its effectiveness therefore depends not only on possessing formal enforcement powers but also on confidence that those powers can be exercised against the government with the same independence expected when regulating private organisations. Babalola's criticism is strongest when framed in these terms: the statutory relationship creates a structural question about perceived and actual autonomy that becomes especially important where the state itself is the controller.

The comparison with the UK is useful, but again should not become an assumption of institutional superiority. The ICO has demonstrated willingness to take enforcement action against central government, including the £500,000 penalty imposed on the Cabinet Office following the New Year Honours data breach. That experience shows why demonstrable independence matters: regulatory autonomy becomes credible through practice, not merely through statutory declarations.

---

[31] ibid 7

The institutional divide identified here is therefore not that the UK possesses an independent regulator while Nigeria does not. The more defensible conclusion is that the credibility of regulatory independence must be demonstrated through transparent and consistent enforcement practice, particularly in cases involving public authorities. For subject access, publication of decisions would serve a dual purpose. It would clarify section 34 while also providing evidence that the Commission's enforcement powers operate independently across both public and private sectors.

The analysis thus moves the effectiveness question beyond the formal availability of remedies. Nigeria already possesses substantial enforcement powers. The more pressing issue is whether judicial interpretation, published regulatory reasoning and demonstrably autonomous enforcement can progressively convert those powers into a predictable body of subject access law. This is where the gap between having a statutory right and having a mature rights regime becomes most visible.

5. Recommendation: From Transplantation to Domestic Operationalisation

The comparison suggests that the principal task facing Nigeria is not the creation of a broader subject access right, but the operationalisation of the right already contained in section 34. The substantive transplant is largely in place. What remains less developed are the standards that determine how that right works, when it encounters delay, cost, administrative burden, competing interests and disagreement over the adequacy of compliance. Further replication of UK or GDPR provisions would therefore address the wrong problem. As Babalola argues more generally, Nigeria's data protection regime requires a distinct identity rather than continued wholesale comparison with the GDPR. The value of a transplanted rule ultimately depends on whether it can function within the receiving legal environment.

5.1. Subject-access-specific regulatory guidance.

The first priority should therefore be subject-access-specific regulatory guidance. The GAID 2025 provides an important general implementation framework, but the issues identified in this study require more precise treatment. A dedicated NDPC instrument could define the circumstances in which identification may be requested, explain how requests made through representatives should be treated, establish expectations for searches and clarify how controllers should deal with mixed personal data. The purpose would not simply be administrative convenience. Where section 34 uses open-ended language, regulatory guidance can reduce the discretion that controllers otherwise exercise in determining the practical boundaries of the data subject's own right.

5.2. Pay Attention to time and search obligations

Particular attention should be given to time and search obligations. The expression ‘unreasonable delay’ offers flexibility but leaves both sides without a sufficiently predictable benchmark. A presumptive response period, coupled with defined grounds for extension, would preserve flexibility while making non-compliance easier to identify. Similarly, the absence of an articulated search standard leaves a crucial aspect of access under-specified. Nigeria need not reproduce the UK's "reasonable and proportionate" formulation, but it requires a standard capable of preventing both extremes: an unrealistic obligation to search indefinitely and a

controller's reliance on a superficial search as evidence of compliance. The issue is one of burden allocation, not linguistic conformity with UK law.

The unreasonable costs proviso in section 34 also requires tighter control. Its present formulation potentially allows the financial burden of access to shift from controller to data subject without specifying when that shift is justified. Regulatory clarification should identify what expenses may properly be regarded as exceptional, require controllers to substantiate any charge and prevent inefficient record management from being converted into a cost payable by the requester. Otherwise, the provision risks making the practical reach of the right dependent not only on the complexity of the request but also on the requester's capacity to pay. That outcome would sit uneasily with the transparency function that section 34 is intended to serve.

5.3. Better Publication of Regulatory Reasoning

A further priority is greater publication of regulatory reasoning. The NDP Act gives the NDPC substantial enforcement powers, but enforcement that remains largely invisible has limited capacity to clarify the law for persons beyond the immediate dispute. The Commission's general investigatory activity does not reveal how contested questions under section 34 are being resolved. Publishing anonymised subject access decisions or structured case summaries would allow standards to develop around delay, searches, costs, exemptions and remedies without requiring every disputed issue to reach the courts. This would also provide evidence of how the Commission exercises its supervisory authority against both public and private controllers.

These reforms should be understood as localisation rather than further transplantation. The aim is not to make Nigerian subject access law look more British. It is to ensure that section 34 answers, within the Nigerian regulatory environment, the practical questions that any effective access regime must confront. This approach is consistent with the wider argument that transplantation is most successful when borrowed rules are adapted to the institutions and conditions in which they must operate. Bridging the divide therefore requires a shift from formal equivalence to operational certainty. Nigeria already possesses the core statutory right and significant enforcement machinery. What it now requires is a body of domestic standards capable of giving that right predictable content. The success of section 34 should ultimately be measured not by how closely it resembles Article 15, but by whether a Nigerian data subject can invoke it knowing with reasonable certainty what the controller must do, when it must do it and what remedy follows when it fails.

6. Conclusion

This article has argued that the principal divide between UK and Nigerian subject access law does not lie in the formal recognition of the right. Section 34 of the NDP Act provides a substantial entitlement that broadly reflects the core protections contained in Article 15 UK GDPR. The more significant distinction emerges when the right is exercised. Questions of response time, cost, search obligations, competing interests and the consequences of non-compliance reveal that substantive convergence has not yet produced equivalent operational certainty.

This finding complicates any simple characterisation of the Nigerian regime as weaker. The NDP Act gives the NDPC significant investigative and remedial powers, including the ability to

compel compliance with data-subject rights. The difficulty is instead that several standards governing section 34 remain open-textured, while subject-access-specific judicial and regulatory interpretation is still limited. As a result, important aspects of the right may depend heavily on the discretion of controllers until those standards are clarified through authoritative guidance, enforcement decisions or litigation.

The comparison with the UK is therefore valuable principally because it demonstrates how a broadly stated access right can acquire practical content through the interaction of legislation, regulatory interpretation and judicial decision-making. It does not establish that Nigeria should reproduce UK rules wholesale. Indeed, the legal-transplant literature cautions against equating similarity to the GDPR with regulatory effectiveness and stresses the importance of adaptation to domestic legal and institutional conditions.

The answer to the central research question is therefore qualified. Nigeria provides a substantively comparable right of access, but the framework governing its practical boundaries remains less developed. Bridging that divide requires less emphasis on further borrowing and greater attention to domestic operationalisation, particularly clearer standards on time, search obligations, costs and competing interests, together with transparent regulatory reasoning. The future effectiveness of section 34 will ultimately depend not on how closely it resembles Article 15, but on how clearly and consistently it is given meaning within Nigeria's own legal and institutional environment.