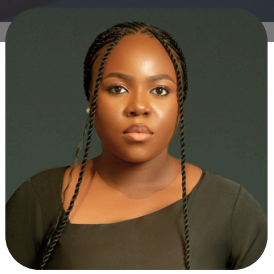
JULY 2026

POLICY TO PRACTICE: LESSONS FROM THE UK'S NEW DATA PROTECTION COMPLAINTS FRAMEWORK



Tolulope Raji
Head, Governance, Data Protection & Digital Transformation



Precious Bassey
Associate Counsel

Executive Summary

The United Kingdom's Data (Use and Access) Act 2025 (DUAA) introduces one of the most significant operational reforms to the UK's data protection framework since Brexit. Among its key reforms is a statutory requirement for organisations that process personal data to establish and maintain a documented data protection complaints procedure by 19 June 2026.

Although the requirement applies directly to organisations subject to UK data protection law, its significance extends beyond the UK. It reflects a broader regulatory trend towards demonstrable accountability, with regulators increasingly expecting organisations to show not only that they have appropriate policies in place, but also that they have effective processes for handling complaints and protecting individuals' rights in practice.
For Nigerian organisations, particularly those involved in cross-border processing, financial services, technology, outsourcing or multinational operations, the reforms offer a useful indication of the direction in which data protection regulation is evolving. While the Nigeria Data Protection Act 2023 (NDPA) and the General Application and Implementation Directive 2025 (GAID) recognise data subjects' rights to seek redress and provide mechanisms for addressing privacy complaints, they stop short of prescribing detailed internal complaints handling procedures in the same way as the UK's new framework.

This article examines the complaints handling requirements introduced by the DUAA, compares them with Nigeria's existing legal framework, and considers the practical lessons for Nigerian organisations, regulators and legal practitioners. It argues that the UK reforms reflect a wider shift from compliance based primarily on documentation towards governance that is embedded in day-to-day organisational practice.

Why complaints mechanisms matter in data protection

At its core, the effectiveness of any data protection regime depends not merely on the rights it recognises, but on the mechanisms available to enforce those rights. While modern privacy legislation typically grants individuals a broad range of protections including rights of access, rectification, erasure, objection and redress, those rights have limited practical value unless they can be exercised through accessible, transparent and effective complaints procedures. Consequently, complaints handling has emerged as a defining feature of mature data protection governance, serving as the bridge between legal obligations on paper and meaningful protection in practice. Increasingly, regulators are recognising that organisational accountability is demonstrated not only by the existence of privacy policies and compliance documentation, but also by the ability to receive, investigate and resolve complaints fairly, consistently and without unnecessary delay.

The DUAA's New Complaints Handling Framework: A Shift Towards Operational Accountability

Under the DUAA, organisations that process personal data are required to establish and maintain a documented complaints procedure that is readily accessible to individuals. The procedure must enable individuals to raise concerns relating to the processing of their personal data and provide a clear mechanism through which those concerns are investigated and resolved.

Beyond prescribing procedural requirements, the reforms reflect an important policy objective. By requiring organisations to establish formal complaints procedures before individuals escalate matters to the Information Commissioner's Office (ICO), the DUAA encourages the early resolution of disputes at organisational level. This approach not only promotes more efficient use of regulatory resources but also incentivises organisations to take greater ownership of their privacy obligations. Rather than viewing complaints as matters to be addressed only after regulatory intervention, organisations are encouraged to embed complaint resolution within their broader governance and risk management frameworks, thereby fostering a culture of accountability and continuous improvement.

Importantly, organisations must acknowledge receipt of a complaint within 30 days and respond without undue delay. Where a complaint is accepted, the organisation is expected to take appropriate remedial action. Where it rejects the complaint or considers that no further action is required, it must explain the reasons for its decision and inform the complainant of their right to escalate the matter to the ICO.

The legislation therefore moves beyond recognising a right to complain. It prescribes how organisations must operationalise that right through documented procedures, defined timelines, appropriate record-keeping and transparent communication. This represents a significant shift in regulatory expectations. Complaints handling is no longer treated solely as a customer service or legal function but as an integral

component of organisational governance and accountability. This represents a notable evolution in regulatory thinking. Historically, privacy compliance was often assessed by reference to whether organisations had adopted the necessary policies, notices and contractual safeguards. Contemporary regulators, however, increasingly expect organisations to demonstrate that these governance arrangements operate effectively in practice. A documented complaints procedure provides tangible evidence that an organisation is capable of identifying potential privacy failures, responding appropriately to individuals' concerns and implementing corrective measures where necessary. In this regard, complaints handling becomes more than an administrative process; it functions as a practical mechanism through which accountability is tested, measured and continually strengthened.

Although these reforms apply directly only within the United Kingdom, their significance extends well beyond the UK's borders. Data protection regulation has increasingly developed through comparative learning, with regulatory innovations in one jurisdiction often influencing governance expectations elsewhere. For jurisdictions such as Nigeria, where accountability already constitutes a fundamental principle of data protection law, the UK's reforms provide a useful opportunity to examine how broad statutory principles may be translated into detailed operational requirements. The comparison therefore extends beyond legislative drafting to broader questions concerning regulatory design, organisational governance and the practical enforcement of privacy rights.

The Position under the NDPA and GAID

Nigeria's data protection framework similarly recognises the right of individuals to challenge the processing of their personal data and seek redress where they believe their rights have been infringed. The NDPA establishes the right of data subjects to lodge complaints with the Nigeria Data Protection Commission (NDPC) and empowers the Commission to investigate complaints, issue compliance directives and impose administrative sanctions where appropriate.

The GAID builds upon these statutory provisions by requiring data controllers and processors to implement measures that facilitate the exercise of data subject rights. Organisations are expected to establish appropriate governance structures, designate responsible officers where required, maintain records of compliance activities and implement mechanisms for responding to requests from data subjects.

However, unlike the DUAA, neither the NDPA nor the GAID prescribes a dedicated internal complaint handling procedure. There is no statutory requirement for organisations to maintain a documented complaints policy, acknowledge complaints within a specified period or communicate prescribed information regarding escalation rights before a complaint is referred to the NDPC.

A Shift from Principles to Operational Governance

The principal distinction between the two frameworks lies not in the recognition of individual rights but in the level of regulatory prescription.

Both jurisdictions recognise accountability as a fundamental principle of data protection. Both require organisations to facilitate the exercise of data subject rights and both empower their respective regulators to investigate complaints and enforce compliance.

The UK reforms, however, take accountability one step further by prescribing the operational processes through which organisations must manage complaints. Rather than leaving organisations to determine their own procedures, the DUAA establishes minimum governance standards that apply across all organisations within its scope.

This reflects a broader international regulatory trend. Increasingly, regulators are moving away from assessing compliance solely by reference to written policies and are instead examining whether organisations have embedded effective governance processes capable of delivering practical outcomes for individuals.

The Nigerian framework already contains many of the building blocks of accountability, including obligations relating to governance, risk management, transparency, record-keeping and data subject rights. The DUAA demonstrates how those principles can be translated into specific operational requirements, providing greater consistency for organisations and clearer expectations for data subjects.

Comparative Analysis of the DUAA and Nigeria's NDPA/GIAD

Issue	United Kingdom (DUAA 2025)	Nigeria (NDPA 2023 & GAID 2025)	Convergence / Difference
Right to complain	Individuals have the right to submit complaints about the processing of their personal data to organisations before escalating the matter to the ICO.	Data subjects have the right to lodge complaints with data controllers and the Nigeria Data Protection Commission (NDPC) where they believe their rights have been infringed.	Convergence: Both frameworks recognise the right of individuals to challenge unlawful or unfair processing.
Internal complaints procedure	Organisations must establish and maintain a documented and accessible data protection complaints procedure.	There is no express statutory requirement to maintain a documented internal complaints procedure, although organisations are expected to facilitate the exercise of data subject rights.	Difference: The DUAA creates a specific legal obligation; the NDPA adopts a principles-based approach.

Accessibility	Complaints procedures must be easy to access and clearly communicated to data subjects.	The NDPA and GAID require organisations to make information available to data subjects, but do not prescribe how complaints mechanisms should be presented.	Difference: The UK imposes a more prescriptive accessibility requirement.
Acknowledgement of complaints	Organisations must acknowledge receipt of a complaint within 30 days.	No statutory timeframe is prescribed for acknowledging complaints.	Difference: The DUAA introduces a mandatory procedural deadline.
Response requirements	Organisations must investigate complaints, provide a reasoned outcome, explain any refusal to act and inform complainants of their right to approach the ICO.	Organisations are expected to respond appropriately to data subject requests and cooperate with the NDPC, but there is no prescribed format or statutory content for complaint responses.	Difference: The UK framework provides considerably greater procedural certainty.
Escalation to the regulator	If dissatisfied with the organisation's response, individuals may complain to the Information Commissioner's Office (ICO).	Data subjects may submit complaints directly to the Nigeria Data Protection Commission (NDPC), which has investigative and enforcement powers.	Convergence: Both jurisdictions provide independent regulatory oversight and enforcement.
Accountability	Complaints handling forms part of an organisation's statutory accountability obligations.	Accountability is a core principle under the NDPA and GAID, requiring organisations to implement appropriate technical and organisational measures.	Convergence: Both frameworks are founded on accountability, although they operationalise it differently.

Governance requirements	Organisations must embed complaints handling within their governance arrangements through documented procedures and record-keeping.	Organisations are expected to establish governance structures appropriate to their processing activities, including privacy management programmes and compliance measures.	Convergence: Both require governance. Difference: The UK prescribes a specific governance process for complaints.
Regulatory approach	Rules-based, with detailed statutory procedural requirements.	Principles-based, allowing organisations greater flexibility in determining how compliance is achieved.	Difference: The UK is more prescriptive, while Nigeria provides greater discretion.
Regulatory objective	To encourage early resolution of complaints, improve accountability and reduce unnecessary referrals to the ICO.	To safeguard data subject rights, promote responsible processing and enable effective regulatory oversight by the NDPC.	Convergence: Both seek stronger protection for individuals and improved organisational compliance.

Practical Implications for Nigerian Organisations

Although Nigerian organisations operating solely within Nigeria are not legally required to adopt the UK's complaints handling framework, the DUAA provides a useful benchmark for strengthening privacy governance. This is particularly relevant for organisations that process personal data across borders, serve UK customers, provide outsourcing or technology services to international clients, or seek to demonstrate robust governance to investors, business partners and regulators.

A structured complaints handling process can deliver benefits beyond regulatory compliance. It enables organisations to resolve privacy concerns promptly, identify recurring compliance issues, reduce regulatory risk and demonstrate accountability where complaints are investigated by the regulator.

Beyond resolving individual grievances, organisations should also establish processes for periodically reviewing complaint trends to identify systemic compliance issues. Regular reporting of privacy complaints to senior management or governing boards can provide valuable insight into emerging risks, recurring operational weaknesses and the effectiveness of existing privacy controls. Integrating complaint analysis into broader governance and risk management frameworks enables organisations to move beyond reactive compliance and towards a culture of continuous improvement, where lessons learned from individual complaints inform policy development, employee training and future compliance strategies.

Equally important is the role of organisational culture. The effectiveness of any complaints framework depends not only upon documented procedures but also upon the willingness of employees to recognise privacy concerns, escalate them appropriately and engage transparently with complainants. Organisations should therefore complement formal procedures with regular staff training, clearly defined reporting responsibilities and visible support from senior management. Embedding these practices across the organisation reinforces accountability and helps ensure that privacy complaints are addressed consistently, fairly and in accordance with regulatory expectations.

While neither the NDPA nor the GAID prescribes a formal internal complaints procedure, organisations should consider adopting governance measures consistent with international best practice. These include:

- implementing a documented complaints handling procedure;
- assigning responsibility for managing privacy complaints;
- maintaining records of complaints, investigations and remedial actions;
- establishing clear escalation and response timelines; and
- training relevant personnel to identify and manage privacy-related complaints effectively.

Although these measures are not mandatory under Nigerian law, they align with the accountability principle underpinning the NDPA and GAID and place organisations in a stronger position to respond to increasing regulatory scrutiny.

Conclusion

The DUAA marks a significant step in the evolution of data protection regulation by making internal complaints handling a statutory component of organisational accountability. Although Nigeria's data protection framework adopts a less prescriptive approach, both regimes share the common objective of protecting data subject rights through effective governance.

For Nigerian organisations, the UK's reforms provide more than a point of comparison. They offer a practical benchmark against which existing privacy governance arrangements can be assessed. Organisations that strengthen their internal complaints handling processes now will be better placed to demonstrate accountability, enhance stakeholder trust and respond to increasingly sophisticated regulatory expectations in both domestic and international markets.

The DUAA demonstrates that the future of data protection regulation lies not simply in recognising individual rights, but in ensuring that those rights can be exercised through effective organisational processes. While the NDPA and GAID adopt a more principles-based approach, they share the same underlying objective of promoting accountability, transparency and respect for data subject rights.

As digital ecosystems become increasingly interconnected and regulatory expectations continue to evolve, organisations that invest in robust complaints handling mechanisms will be better positioned to demonstrate compliance, strengthen stakeholder confidence and respond effectively to emerging privacy risks. Ultimately, the true measure of a mature data protection framework is not the breadth of rights recognised in legislation, but the effectiveness of the institutional and organisational processes that enable those rights to be realised in practice.

Key References

United Kingdom
• Data (Use and Access) Act 2025.
• UK General Data Protection Regulation (UK GDPR).
• Data Protection Act 2018.
• Information Commissioner's Office (ICO), Guidance on Data Protection Complaints Procedures.
• ICO Consultations on Recognised Legitimate Interests and Complaints Handling (2025).
Nigeria
• Nigeria Data Protection Act 2023.
• Nigeria Data Protection Commission, General Application and Implementation Directive 2025.
• Constitution of the Federal Republic of Nigeria 1999 (as amended), section 37.
• Fundamental Rights (Enforcement Procedure) Rules 2009.
• Relevant enforcement decisions and guidance issued by the Nigeria Data Protection Commission.

Disclaimer

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