Shaping Nigeria's Sectoral Data Protection Regimes: Insights from the UK Data (Use and Access) DUAA, 2025

www.strenandblan.com
contact@strenandblan.com
@strenandblan

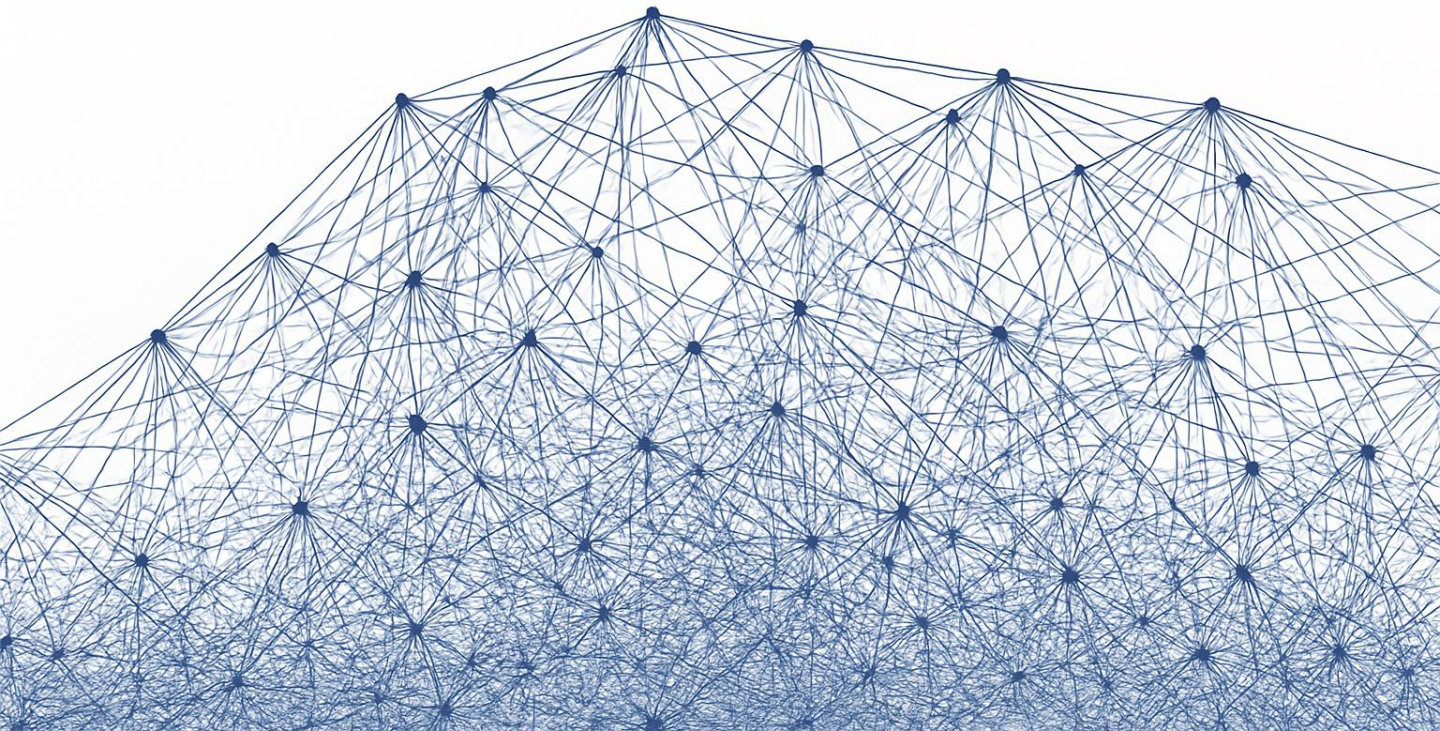
+234 (0)702 558 0053
3 Theophilus Orji Street, Off Fola Osibo Road, Lekki Phase 1, Lagos, Nigeria

10th September 2025

Introduction

Data has become the defining asset of the digital economy, shaping how services are delivered and how innovation is achieved across sectors such as finance, healthcare, telecommunications, energy, and transportation. This central role of data has also heightened concerns around misuse, security breaches, and the erosion of consumer trust. While general data protection laws provide a foundational framework, they often fall short of addressing the sector-specific realities and risks that arise in practice.

Different industries interface with data in different ways, and as such, a one-size-fits-all approach is no longer sufficient. The United Kingdom has sought to bridge this gap through the enactment of the Data (Use and Access) DUAA 2025 (the "**DUAA**"), a landmark law that refines UK GDPR, enables "Smart Data" schemes, promotes digital verification services, and modernises rules on research, cookies, and international transfers. By going beyond broad principles and introducing tailored obligations for specific sectors, the DUAA not only strengthens the protection of data subjects but also supports innovation and efficiency within regulated industries. This article examines the key features of the DUAA, its sectoral applications, and what lessons Nigeria can draw as it considers the development of sector-specific frameworks. It also reflects on Nigeria's current regulatory posture and offers practical recommendations for regulators, navigating the country's evolving data protection landscape.



Overview of the UK Data (Use and Access) DUAA 2025

The DUAA represents one of the most significant updates to the United Kingdom's digital regulatory landscape since the introduction of the General Data Protection Regulation (GDPR). Rather than replacing the existing regime, the DUAA strategically amends and supplements key statutes, including the GDPR, the Data Protection DUAA 2018, and the Privacy and Electronic Communications Regulations (PECR). By doing so, it ensures continuity with established frameworks while introducing reforms designed for the realities of today's data-driven economy. At its core, the DUAA seeks to improve the way data can be accessed, shared, and used across industries in a manner that safeguards individual rights while fostering innovation that increases economic and social value. [1]

Key Innovations Under the UK Data (Use and Access) DUAA 2025

A defining feature of the DUAA relevant to our discourse is the introduction of tailored provisions across various sectors of the economy. Rather than treating data protection frameworks as a one-size-fits-all regime, the DUAA recognises the distinct challenges of diverse industries. By doing so, the DUAA sets out a more flexible and innovation-friendly framework while maintaining core safeguards for data subjects. For Nigeria, where sector-specific data use and protection frameworks are yet to fully take shape, these provisions under the DUAA offer valuable insights into how data protection frameworks can be designed to support industry growth without compromising accountability. The following areas highlight the key sector-by-sector reforms introduced under the DUAA and the implications for companies operating in these areas.

1 Understanding the Data (Use and Access) DUAA 2025, https://www.360lawservices.com/blog/understanding-the-data-use-and-access-DUAA-2025/ [Accessed 4th September 2025].

1. Health and Life Sciences

The DUAA introduced far-reaching reforms for the health and life sciences sector. One of the most significant innovations is the relaxation of rules around data sharing within the National Health Service (NHS), [2] allowing easier movement of patient data between hospitals, general practitioners, and ambulance services. For companies within this sector, this innovation brings new opportunities for collaboration in research and clinical trials, supported by clearer rules on when data can be shared. The DUAA also strengthens the lawful basis for processing personal data in emergencies or where vulnerable individuals must be protected, through its "recognised legitimate interests" provision. This provision relaxes the traditional balancing test, making it easier for organisations to respond quickly in high-risk situations. Nigeria's healthcare sector is heavily fragmented, with data often siloed between federal institutions, state ministries of health, and private providers. Although the Nigeria Data Protection Act (NDPA) provides general data protection standards, no sector-specific provisions guide the sensitive handling of health data. Furthermore, data sharing across hospitals or states in the event of a medical emergency is still a challenge. Adopting a framework similar to the DUAA could support interoperability in Nigeria's health system while also creating stronger safeguards around the processing of patient data.

2. Financial Services and Digital Identity

The DUAA also makes key provisions for the financial services sector, particularly through its expansion of Smart Data schemes. Building on the success of open banking, the DUAA provides a legal framework that allows similar data portability and interoperability schemes to be extended to other industries, including utilities and property services. For financial institutions, this creates opportunities to design new customer-centric products powered by secure data sharing. In addition, the DUAA establishes a framework for digital verification services, complete with a government-endorsed trust mark and an accreditation system for providers. [3] This has direct implications for banks, fintechs, and other regulated institutions, as it provides an avenue for secure, scalable identity verification systems that reduce fraud and enhance consumer confidence. Companies operating within this sector will need to consider how best to integrate these tools into their service delivery and compliance structures. Nigeria's financial sector is among the most data-driven, with fintechs, banks, pension funds, and insurers all reliant on customer data for service delivery. Oversight, however, is split between the Nigerian Data Protection Commission (NDPC) and the Central Bank of Nigeria (CBN), often leaving businesses to interpret overlapping obligations. While CBN has issued cybersecurity and data privacy directives, there is still no comprehensive sector-specific framework that harmonises these rules with the NDPA. A DUAA-style approach could give Nigeria's financial industry clearer guidance while supporting fintech innovation and consumer protection.

2 What the Data (Use and Access) DUAA 2025 means for your sector, https://harperjames.co.uk/article/data-use-access-DUAA-2025-sector-impDUAA/ [Accessed 5th September 2025].
3 Section 50 of the DUAA

3. Scientific Research and Academia

Another major innovation lies in the area of research. The DUAA broadens the scope of what qualifies as "scientific research" by explicitly including commercially funded and private initiatives. [4] Researchers may now rely on broad consent where it is not possible to define the precise scope of a project at the outset. Furthermore, organisations are now permitted to reuse data for new research purposes without issuing fresh privacy notices, provided that doing so would involve disproportionate effort. This innovation is particularly beneficial for universities, research institutes, and private laboratories, which often grapple with the challenges of secondary use of data. By creating a clearer framework, the DUAA creates more room for innovation within this sector while maintaining safeguards against misuse. In Nigeria, most research institutions and universities handle large volumes of personal and scientific data but face structural and regulatory bottlenecks in leveraging data for innovation. The NDPA does not currently contain research-specific provisions, leaving institutions to rely on general lawful bases. Introducing research-focused exceptions, as seen in the DUAA, could boost Nigeria's capacity for healthtech, agri-tech, and other research-intensive industries while still safeguarding ethical standards.

4. Artificial Intelligence (AI) and Automated Decision-Making

The DUAA also addresses the increasing use of AI and automated decision-making (ADM) across multiple sectors. Under the previous regime, strict limitations made it difficult for organisations to rely solely on automated tools in contexts such as recruitment, credit scoring, or customer profiling. The DUAA introduces a more flexible framework that permits ADM, provided that certain safeguards such as transparency, avenues for appeal, and human oversight are in place. [5] This approach reflects a pragmatic recognition of the central role AI now plays in service delivery. At the same time, the DUAA continues to prohibit certain forms of automated processing, especially where sensitive personal data is involved. For companies deploying AI, the implication is that while regulatory flexibility has improved, investment in oversight structures and clear governance mechanisms remains non-negotiable. While the NDPA recognises ADM, there are no detailed provisions tailored to the realities of AI deployment. Oversight currently falls across different regulators, with the Nigeria Data Protection Commission (NDPC) handling data rights and the National Information Technology Development Agency (NITDA) advancing a National AI Strategy. However, the absence of a unified, sector-specific framework leaves businesses uncertain about compliance expectations. Drawing from the DUAA, Nigeria could benefit from clearer lawful bases for ADM, industry-specific safeguards, and stronger guidance on issues such as algorithmic accountability, bias, and redress mechanisms.

4 Section 67(2) of the DUAA
5 Section 80 of the DUAA

5. Digital Services and Marketing

In the digital services and marketing sector, the DUAA introduced a more business-friendly e-privacy framework. It removed the requirement for explicit consent for certain low-risk cookies, such as those used for analytics or service functionality, as long as users are informed and given simple opt-out options. This reduces friction for online platforms and retailers, many of which previously struggled with high drop-off rates due to intrusive cookie banners. Nigeria's telecom and digital services sector is overseen by the Nigerian Communications Commission (NCC) but lacks a full-fledged data protection framework. Given the massive volume of personal data processed by mobile networks, Internet Service Providers, and digital platforms, the absence of sectoral standards creates regulatory gaps. Drawing from the DUAA, Nigeria could develop rules that specifically address telecoms, digital advertising, and AI-driven services, protecting individual rights while encouraging the growth of its digital economy.

Insights into Nigeria's Current Posture on Sector-Specific Data Protection Frameworks

Nigeria has taken notable steps toward modernising its data protection regime with the enactment of the NDPA, which established the NDPC as the primary regulator of data controllers and processors. The subsequent release of the General Application and Implementation Directive (GAID) provided further guidance on how the NDPA should be interpreted and enforced. In line with this mandate, NDPC recently signalled a sector-focused approach to regulation. Through a public notice issued on 25th August 2025, [6] NDPC announced the commencement of sector-by-sector investigations targeting insurance companies, pension managers, gaming operators, banks, and insurance brokers, to assess compliance with the NDPA across these industries. However, despite this promising direction, Nigeria has yet to develop dedicated sector-specific frameworks or guidelines that clearly define how industries should address their unique data protection challenges.

The absence of these distinct frameworks is costly. For businesses, the lack of tailored guidance creates uncertainty about regulatory expectations, complicating compliance efforts. It also encourages fragmentation, as overlaps between the NDPC and other sectoral regulators such as CBN and NCC may lead to conflicting obligations. Enforcement is also weakened, as the NDPC lacks clear benchmarks against which to measure industry-specific compliance. Additionally, Nigeria risks missing out on opportunities. Countries that move early to implement smart, sector-sensitive data frameworks often give their businesses a competitive edge in high-growth areas such as fintech, healthtech, and digital services.

6 NDPC begins sectoral investigations into data protection violations, https://businessday.ng/news/article/ndpc-begins-sectoral-investigations-into-data-protection-violations/ [Accessed 6th September 2025].

Recommendations for Nigeria's Sector-Specific Data Protection Frameworks

Looking ahead, Nigeria has an opportunity to strengthen its data protection regime by adopting frameworks that are tailored to the unique realities of different industries. The following recommendations are worth considering:

1. Development of sector-specific guidelines

To reduce uncertainty and provide clarity for businesses, the NDPC should spearhead the development of sector-specific guidelines in partnership with relevant industry regulators such as the CBN and the NCC. Establishing joint working groups or similar mechanisms would allow these regulators to pool expertise, harmonise requirements, and design frameworks that are both practical and consistent across various industries. This collaborative approach would prevent overlaps, minimise conflicting obligations, and ensure that sectoral rules reflect the realities of each industry while aligning with Nigeria's broader data protection objectives.

2. Encourage innovation-friendly provisions:

The NDPC can consider introducing lawful bases and exceptions that facilitate critical activities such as medical research, fintech growth, or emergency response. Drawing inspiration from the DUAA, such provisions can be crafted to give industries the flexibility they need to be innovative while maintaining safeguards for the rights of data subjects.

3. Build enforcement capacity:

The effectiveness of sector-specific frameworks depends on the regulator's ability to enforce them. The NDPC should therefore invest in staff training, industry-specific audit tools, and monitoring mechanisms that enable it to oversee compliance effectively across diverse sectors.

4. Promote stakeholder engagement

Widespread consultation with businesses and consumer associations is essential to designing rules that strike the right balance between protecting individual rights and enabling industry growth. An engagement of this kind would not only strengthen compliance but also foster public trust in Nigeria's data protection system.

5. Establish Benchmarks against global best practices:

Studying and adapting lessons from leading jurisdictions such as the United Kingdom, where sectoral data frameworks are already shaping the digital economy, is paramount. Aligning with international standards will not only improve regulatory clarity but also help Nigerian businesses remain competitive in cross-border markets.

Conclusion

The DUAA demonstrates how data protection frameworks can evolve beyond general rules to address the distinct realities of diverse sectors. By creating flexibility for these industries, the DUAA not only strengthens compliance but also creates room for innovation. Nigeria, through the NDPA, GAID and the efforts of the NDPC, has already laid the foundation. However, without sector-specific frameworks, the country risks leaving businesses uncertain, consumers unprotected, and innovation stifled. The NDPC's recent move toward sectoral investigations signals the right direction, but further clarity with tailored frameworks is essential. Adopting a sector-sensitive approach would allow Nigeria to balance accountability with innovation, strengthen public trust, and position its industries to compete in the global digital economy. In essence, the lesson from the DUAA is clear: a sector-specific data protection regime is not only a compliance tool but also a catalyst for growth. For Nigeria, the priority now lies in translating intention into action through timely and decisive regulatory measures.

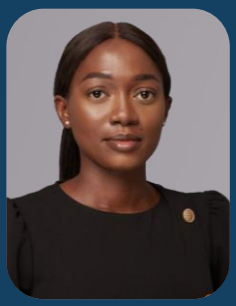
About **Stren & Blan Partners**

Stren & Blan Partners is an innovative and dynamic Law Firm with a compelling blend of experienced lawyers and energetic talents. We are focused on providing solutions to our client's business problems and adding value to their businesses and commercial endeavours. This underpins our ethos as everything we do flows from these underlying principles.

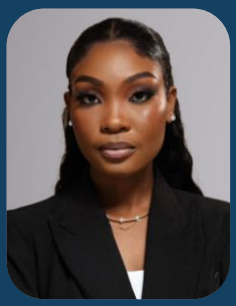
Stren & Blan Partners is a full-service commercial Law Firm that provides legal services to diverse local and multinational corporations. We have developed a clear vision for anticipating our client's business needs and surpassing their expectations, and we do this with an uncompromising commitment to Client service and legal excellence.

The **Authors**

Francisca Igboanugo
Team Lead
FranciscaIgboanugo
@strenandblan.com



Oghenemega Igbru
Associate
OghenemegaIgbru
@strenandblan.com



Eniola Alayo
Associate
EniolaAlayo
@strenandblan.com

+234 (0)702 558 0053
3 Theophilus Orji Street, Off Fola Osibo Road,
Lekki Phase 1, Lagos, Nigeria

www.strenandblan.com
contact@strenandblan.com
@strenandblan