#AdLegal

Insight:

INTEGRATING COMPETITION LAW AND DATA PROTECTION IN UGANDA'S DIGITAL ECONOMY

November 2025

Like all other #AdLegal publications, this report can be downloaded free of charge from the #AdLegal website: **www.adlegalug.com**

Authors:

Aziz Kitaka
Member, AdLegal

Contact:
ed@adlegalug.com

Patience Ayesigye
Member, AdLegal

Contact:
patience@adlegalug.com

Luke Kamoga
Member, AdLegal

Contact:
luke@adlegalug.com

For a long time, data privacy and competition have been treated separately. Privacy laws aim to protect people's data, while competition laws prevent monopolies and encourage fair business practices. But now, these areas overlap. The way a company gathers and uses data influences both privacy and market competition.
Data enables companies to control markets and user interactions, this if misused stifles innovation, limits consumer choices, and poses privacy threats.

In Uganda's digital economy, data has become a key driver of innovation and growth. It enables businesses to create new ideas, improve services, and tailor products to consumer needs. Yet, this same data strengthens the dominance of large technology and service companies operating within the country and across the region.
These digital and service giants such as MTN, Airtel, SafeBoda, Jumia, Online Banking services use advanced technology and vast amounts of user data to consolidate their market positions. Their dominance raises serious questions about both data privacy and fair competition in Uganda's fast-evolving digital landscape.

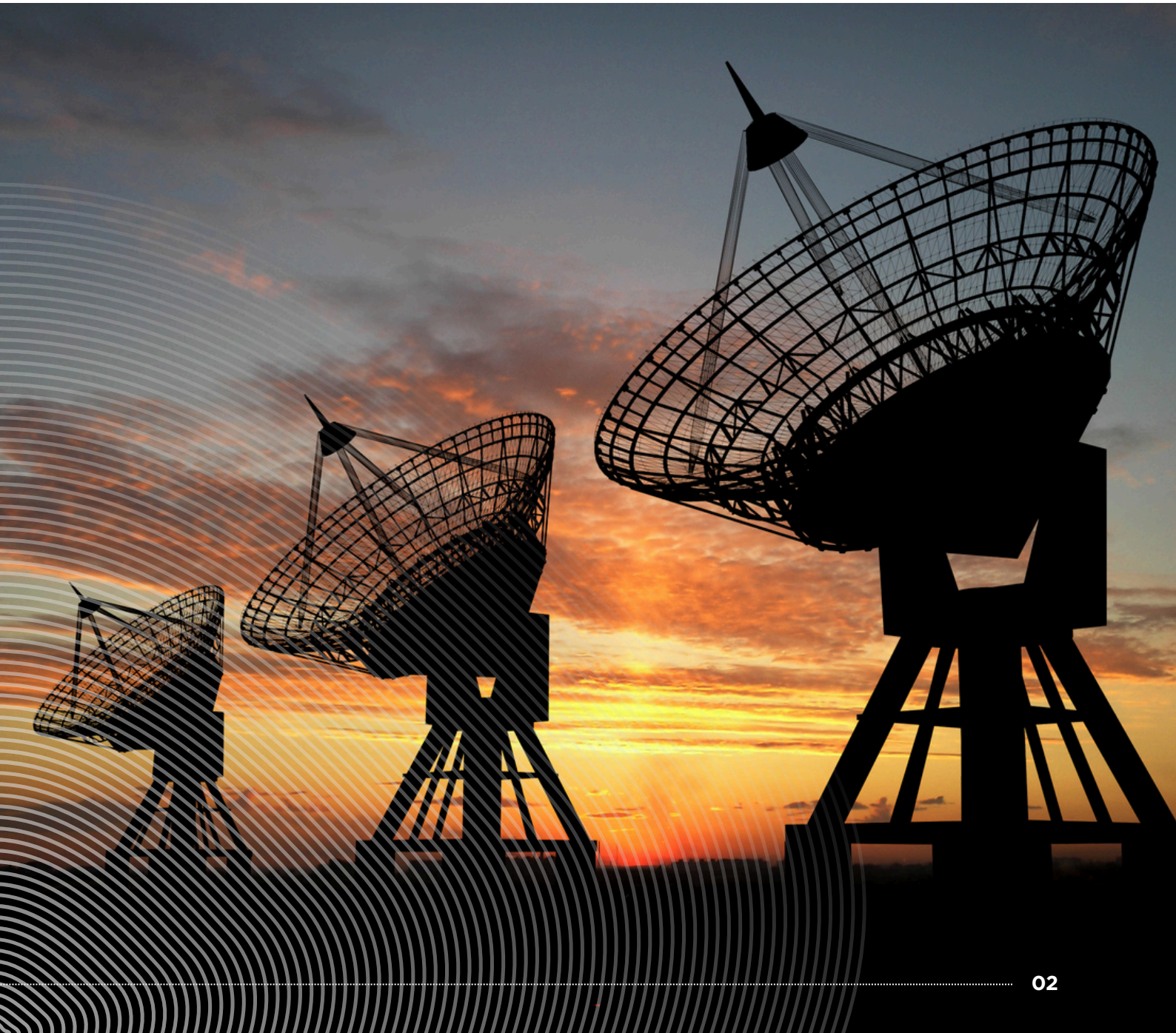
Privacy laws like the **Data Protection and Privacy Act, 2019** and its **Regulations** aim to protect individuals' personal information, while the **Competition Act Cap. 66** and its **Regulations**, are designed to prevent monopolies and encourage fair competition. Increasingly, however, these two areas overlap. How a company collects, processes, and uses data affects not just privacy, but also market fairness.

For example, MTN Mobile Money and Airtel Money collect vast amounts of user data, covering spending patterns, transaction histories, and even location data. This information allows them to launch new digital financial products and offer targeted promotions. However, because they already dominate Uganda's mobile money sector, their ability to exploit user data gives them a competitive edge that smaller fintech companies can hardly match.

The same dynamic can be seen in other sectors. SafeBoda, for instance, gathers detailed trip data from both riders and passengers, enabling it to optimize routes and predict demand. Jumia collects consumer data from online shopping habits to fine-tune product recommendations and delivery efficiency. Banks like Stanbic Bank, Centenary Bank etc use big data analytics to assess creditworthiness and customize banking products.
Over time, their accumulated data creates a self-reinforcing advantage, making their services better while creating barriers for new entrants.

Traditional competition frameworks, which mainly focus on prices and market share, do not fully capture these realities. Many online and digital services appear “free,” yet consumers pay with their personal data. When a company accumulates enough data to influence markets or restrict consumer choice, it harms competition even if prices don’t rise.

In today’s Uganda, data is not just a byproduct of technology, it’s a powerful asset. Those who control it, from telecoms and ride-hailing platforms to e-commerce and financial institutions, enjoy a “data advantage.” This allows them to innovate faster, use AI more effectively, and make more informed decisions. However, it also risks entrenching their dominance, making it difficult for smaller or new businesses to compete posing a challenge that Uganda’s legal and regulatory frameworks must urgently address.



THE LINK BETWEEN COMPETITION LAW AND DATA PRIVACY

The more data a company collects, the better it can personalize its services, attract more users, and in turn, gather even more data, a self-reinforcing cycle that strengthens its dominance. This can easily transform into a competition problem when dominant firms impose unfair terms or conditions simply because users have no real alternatives. These realities show that data privacy and market competition are deeply intertwined. How a company handles user data affects not just individual privacy rights but also the overall fairness and openness of Uganda's digital markets.

Therefore, the overlap between privacy protection and competition law calls for strong coordination between the *Personal Data Protection Office (PDPO)* and the *Committee on Competition and Consumer Protection* under the *Ministry of Trade, Industry and Cooperatives.* Together, these bodies must ensure that data-driven business models promote innovation and consumer benefit without compromising user privacy or market competitiveness.

Does the current legal regime support cooperation between the Personal Data Protection Office (PDPO) and the Ministry of Trade's Technical Committee on Competition and Consumer Protection?

The current legal framework expressly supports cooperation between the Personal Data Protection Office (PDPO) and the Ministry of Trade's Technical Committee on Competition and Consumer Protection. **Regulation 6(1) of the Data Protection and Privacy Regulations, 2021** provides that "the Office shall cooperate with other government ministries, departments and agencies in the implementation of the Act and regulations," while **Regulation 6(2)** requires that "all ministries, departments and agencies of government shall accord to the Office such assistance as may be necessary to ensure proper discharge of its functions." These provisions legally enable joint investigations, information exchange, and policy coordination between the PDPO and the Ministry of Trade in overlapping areas such as data-driven market dominance, consumer profiling, and digital platforms. Additionally, **Section 6** of the **Competition Act Cap. 66** creates a procedural bridge by requiring that where a statutory authority (such as the PDPO) is handling a matter likely to affect competition, it "shall refer the matter to the Ministry," and the Ministry must give its opinion before a final decision is made. Furthermore, **Section 8(c) of the Competition Act** mandates that "the Ministry shall, so far as practicable, cooperate with a body established under any other law, to promote and regulate competition." The phrase "any other law" includes domestic legislation such as the Data Protection and Privacy Act, 2019, thereby legitimizing cooperation with the PDPO.

Taken together, these provisions form a coherent legal basis for coordinated action, mutual assistance, and joint investigations between the two institutions.

However, Practical and legal safeguards, institutional gaps and the absence of an explicit joint-investigation procedure mean cooperation is possible now but would work better with clear protocols (MoUs), statutory clarifications, and operational safeguards.

THE RECENT APPROACH BY NIGERIA:

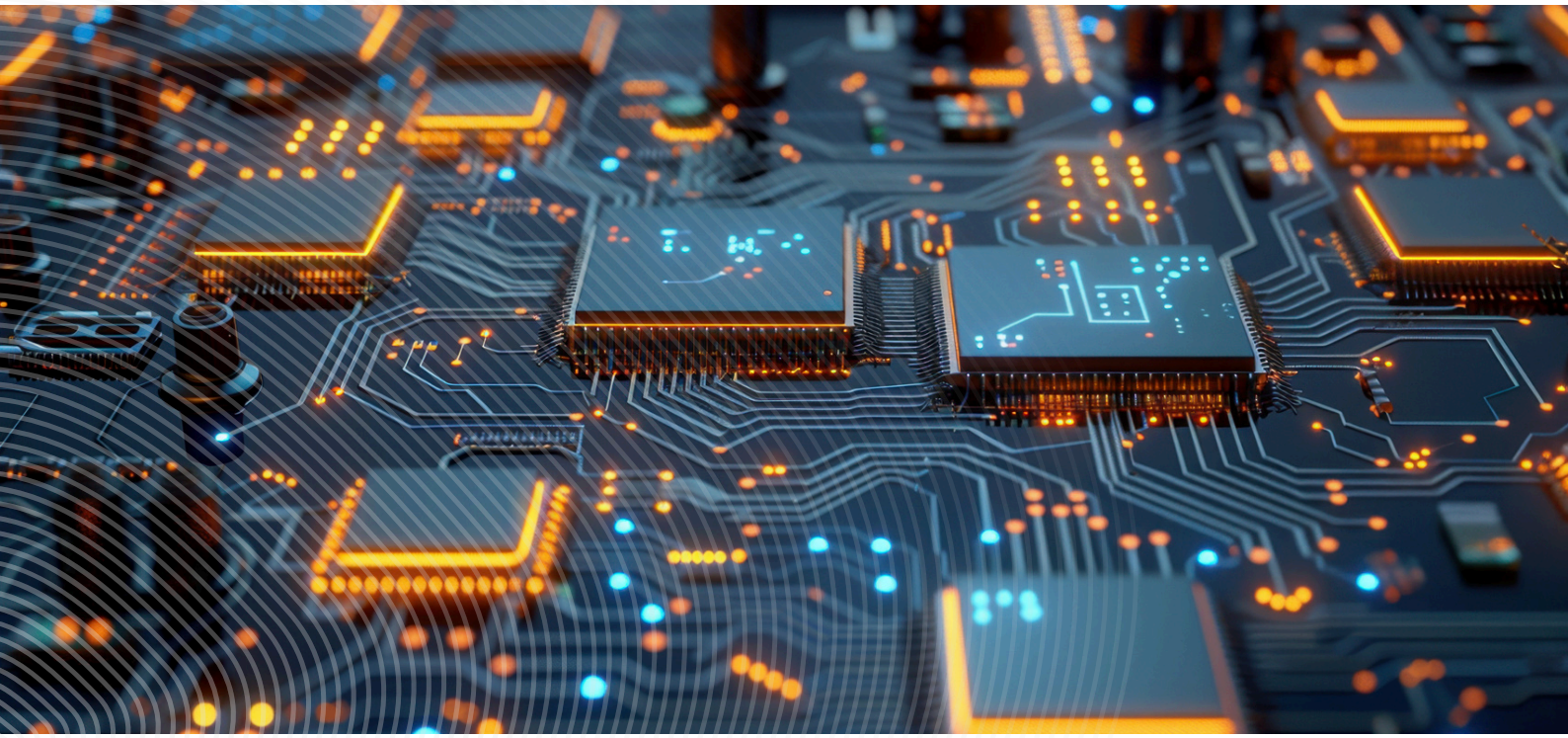
Nigeria provides a practical precedent for inter-agency cooperation between data protection and competition authorities. Under the **Federal Competition and Consumer Protection Act, 2018 (FCCPA)** and the **Nigeria Data Protection Regulation, 2019 (NDPR),** the *Federal Competition and Consumer Protection Commission (FCCPC)* and the *Nigeria Data Protection Commission (NDPC)* formally recognized the intersection between data practices and competition dynamics.

In May 2021, the two agencies jointly initiated an investigation into WhatsApp's updated privacy policy, which sought to compel data sharing with Facebook and its affiliates. The investigation was premised on the understanding that such data practices not only raised privacy and consumer protection concerns but also had potential anti-competitive implications, such as reinforcing market dominance through control of user data.

> **Nigeria provides a practical precedent for inter-agency cooperation between data protection and competition authorities.**

Another noteworthy aspect in this regard is that the investigation conducted by the FCCPC received substantial technological support from the Nigerian National Information Technology Development Agency (NITDA).

This joint regulatory action demonstrated Nigeria's progressive model of cross-sectoral enforcement, where competition and data protection authorities cooperate to address complex digital market issues. It manifests how regulatory synergy can strengthen consumer welfare, ensure accountability of digital platforms, and provide a unified approach to emerging challenges in the data-driven economy.



HOW AND WHY BUSINESSES USE CONSUMER DATA

When examining how businesses collect consumer data in Uganda's growing digital economy, it is important to distinguish between **first-party** and **third-party** data collection. **First-party data** is information a business collects directly from its own customers or users, for example, when a bank like Stanbic Bank Uganda Limited gathers client details through its mobile app or when an online store like Glovo records purchase history. On the other hand, t**hird-party dat**a is collected by companies that are not directly connected to the consumer.

This often happens when businesses use tracking technologies provided by other companies, such as online advertisers or analytics firms, under commercial agreements that allow them to monitor user behaviour or access advertising tools and Application Programming Interfaces (APIs).

Online tracking technologies have also become more advanced in Uganda, as more people use smartphones and digital services. Traditionally, **cookies** were used to track how people browse websites on computers. **First-party cookies** come from the website a person is visiting, while **third-party cookies** come from other, unrelated sites whose content (such as ads or social media plugins) appears on the page. However, cookies are less effective on mobile phones because many mobile browsers block third-party cookies by default and apps often do not share them.

To overcome these challenges, many businesses now rely on **tracking pixels.** These are tiny, invisible images embedded in websites or emails that send a signal back to the server when a page is opened or an email is read. Just like cookies, pixels help track user activity for example, whether a person opened an advert or clicked on a link. This allows companies in Uganda's digital market to build consumer profiles, measure marketing effectiveness, and deliver targeted advertisements, though it also raises important questions about data protection and consumer privacy under Uganda's Data Protection and Privacy Act, 2019.

Lock-In and Network Effect

The lock-in effect refers to a situation where consumers find it difficult to switch from one digital service provider to another because doing so comes with significant inconvenience or costs. In Uganda, this is increasingly evident in sectors like mobile money, telecommunications, and digital payments, where dominant players such as MTN Mobile Money and Airtel Money have created deeply entrenched ecosystems.

For instance, a typical mobile money user may have been using MTN Mobile Money for years saving contacts, receiving salaries, paying bills, and transacting with a wide network of family members, friends, and business partners. Over time, this builds a strong web of interdependence. If that user decides to switch to another platform, such as Airtel Money or a smaller fintech service, they risk losing the convenience and network built on MTN's system. Many of their regular contacts may not be using the alternative service, making it practically difficult to move without losing essential connections or incurring extra transaction costs.

This phenomenon creates network effects, where the usefulness of a platform increases as more people use it. Because nearly everyone from boda riders to market vendors and employers uses MTN or Airtel Mobile Money, new users are naturally drawn to the same platforms. The more people join, the more entrenched the platforms become, reinforcing their dominance.

In such circumstances, consent to the terms and conditions imposed by these platforms becomes questionable. When users are required to agree to extensive data-sharing arrangements as part of continued service, they often have little genuine choice. Declining the terms might mean losing access to vital mobile money functions such as sending or receiving funds, buying airtime, or paying utility bills, activities that have become part of daily life in Uganda's digital economy.

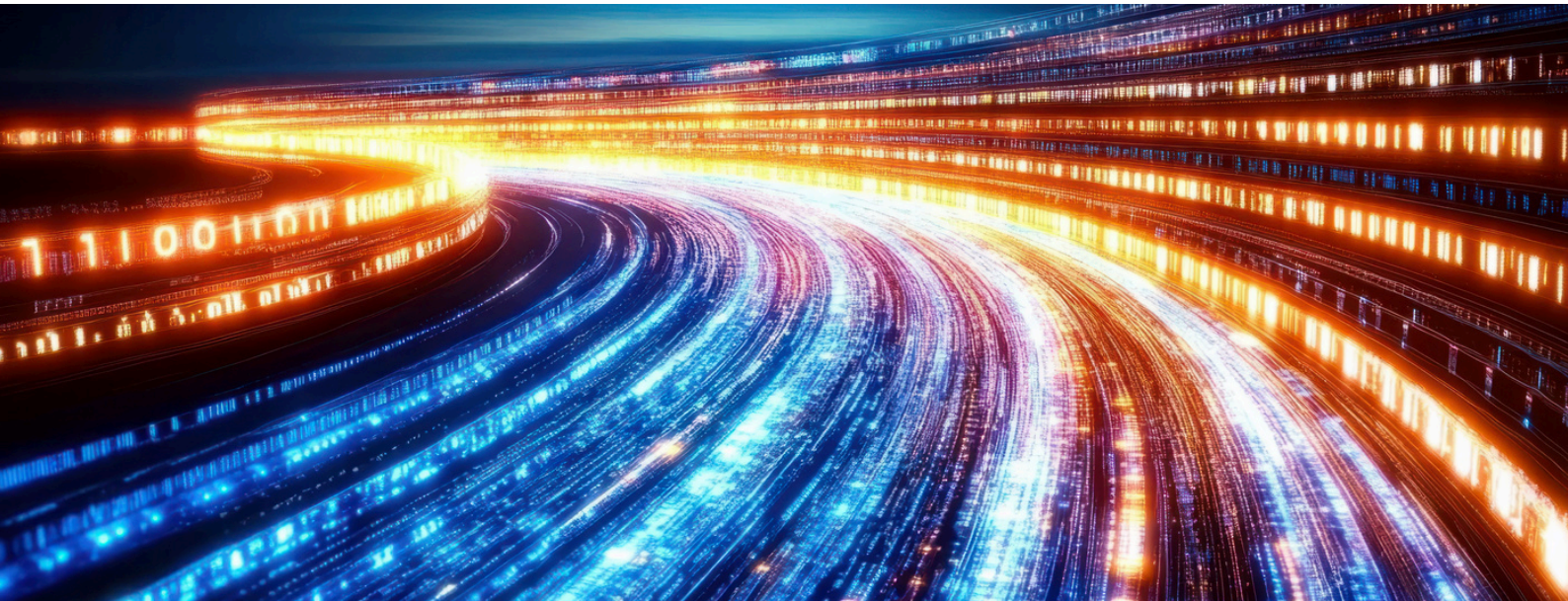
From a competition law standpoint, the concern is not only about how personal data is processed, but whether users have real freedom of choice. Uganda's Competition Act, 2023 empowers regulators to examine whether dominant platforms are abusing their market position for example, by tying essential financial services to intrusive data-sharing requirements or by setting terms that smaller competitors cannot match.
The *Data Protection and Privacy Act, 2019* also plays a complementary role by ensuring that personal data collected through mobile money transactions is used fairly and lawfully. However, the overlapping nature of data power and market power means that collaboration between the *Personal Data Protection Office (PDPO)* and the Competition and the Committee on Competition and Consumer Protection under the Ministry of Trade is essential.

In essence, the lock-in and network effects seen with MTN and Airtel Mobile Money demonstrate how dominant digital platforms in Uganda can make it hard for consumers to switch or meaningfully decline certain terms. This concentration of users and data not only discourages entry by smaller fintech players but also heightens privacy risks — showing why competition and data protection must be treated as interlinked elements of Uganda's digital policy and regulation.

RECOMMENDATIONS

Closer collaboration between the Personal Data Protection Office (PDPO) and the newly established Ministry of Trade's Technical Committee on Competition and Consumer Protection is crucial for building a coherent and future-ready regulatory framework in Uganda's digital economy. As data increasingly underpins both economic competitiveness and individual rights, coordination between these two institutions will be vital in ensuring balanced oversight of data-driven markets. The Technical Committee, in its emerging role, should work closely with the PDPO to address overlapping issues such as data-enabled market dominance, consumer profiling, and digital platform regulation.

Decisions, pronouncements, and actions taken by the PDPO or the Technical Committee including complaint determinations, enforcement directives, or investigation outcomes will shape the practical application of both data protection and competition law. These decisions may lead to appeals or litigation, and in turn, the judiciary will interpret the legal framework and provide guidance on the interface between privacy and competition issues. Collectively, the regulators' rulings and the courts' judgments will create a body of practice that clarifies whether certain privacy violations can amount to anti-competitive conduct. Lessons from global jurisprudence, particularly from the European Union and United States, can further inform these decisions and strengthen Uganda's regulatory approach.



#AdLegal

CONNECT WITH US:

Adlegal International Limited
P.O Box 173818, Kampala
info@adlegalug.com
+256 758 723 991/+256 762 810949
www.adlegalug.com