

Data Monetization

Ownership, Control and
Legal Considerations



Introduction

Digital platforms, artificial intelligence and data analytics have made data an increasingly valuable commercial asset. A 2024 industry report estimated the global data monetisation market at US\$4.84 billion and projected that it would reach US\$12.59 billion by 2029.[1]

Data monetisation is broader than the sale of customer information. It includes the use of data to improve internal decisions, develop analytical products, personalise services, licence market insights or train artificial intelligence systems.

The commercial opportunity is significant, but economic value does not necessarily translate into a legal right to exploit data. Businesses must consider the rights attached to the data, the purpose for which it was collected, the interests of affected individuals and the terms on which it may be shared. A sustainable data-monetisation strategy therefore requires intellectual-property analysis, lawful data processing, effective risk management and carefully structured commercial agreements.

Data Monetization as a Commercial Strategy

Data monetisation may be direct or indirect. Common contexts for indirect monetisation include where a business uses data internally to improve pricing, inventory management, fraud detection, logistics, customer retention or product development. The value appears through increased revenue, lower costs or better decisions rather than through a separate sale.

Direct monetisation involves offering data or data-derived products to third parties. This may take the form of a licence, subscription, industry report, benchmarking service, dashboard, data feed or Application Programming Interface (API). Businesses may also enter into partnerships under which data or insights are combined to support a joint product.

The distinction matters because each model creates a different risk profile. An aggregated industry report will not raise the same issues as the transfer of individual transaction records. A controlled dashboard may allow a business to retain stronger oversight than delivering a complete dataset to a customer. A licence to use data for market research will not necessarily cover model training or the creation of a competing product. The legal and technical structure should therefore follow the commercial objective. Before attempting to monetise a dataset, the business should determine what value it intends to create, who will receive that value and whether the same result can be achieved with less or less sensitive information.

[1]Data as a Strategic Asset | Deloitte US. (2025). Deloitte.
<https://www.deloitte.com/us/en/services/consulting/articles/data-strategic-asset.html>

Access to data does not equate ownership of data. Use and exploitation of purchased data is still subject to the restrictions the seller of the data is subject to... The legal analysis should therefore identify each relevant layer of rights: rights in the database or compilation, rights to access and use the underlying data, confidentiality obligations, data-protection requirements and any sector-specific restrictions.



Legal Control of Data as a Bundle of Rights – Ownership and Risk Considerations

References to “data ownership” can be misleading because Nigerian law does not treat data as a single category of property carrying one comprehensive ownership right.

From a strict legal standpoint, “mere data” or unorganised data generally is not eligible for copyright under the Copyright Act 2022. The intellectual property rights attached to data instead stems from compilations, original database structures and contractual restrictions. An original database or compilation may qualify as a literary work where sufficient effort has been applied to give it an original character and it has been fixed in a medium. However, *Section 2(5) of the Copyright Act 2022* makes clear that copyright in a compilation does not confer an exclusive right over the pre-existing material or data contained in it.^[2] The distinction is important. Copyright may protect the selection, structure or arrangement of a database without preventing another person from lawfully obtaining and using the underlying facts. Similarly, copyright in an analytical report will not necessarily create ownership of every data point used to prepare it.

Commercial control may instead arise from a combination of legal and practical protections. Contracts may restrict use and onward disclosure. Confidentiality obligations may protect information that is not publicly available. Access controls may limit who can retrieve or extract a dataset. Sector-specific rules may restrict the use of financial, health, telecommunications or other regulated information.

Personal data is subject to a further layer of regulation. The Nigeria Data Protection Act 2023 does not create a general property right in personal data for either the individual or the company processing it. Instead, it gives data subjects rights in relation to processing and imposes obligations on data controllers and processors. A business does not therefore acquire an unrestricted right to commercialise personal data simply because the information was generated through its platform, equipment or services. It may control the relevant system and hold contractual or intellectual-property rights in its database while still being restricted in how the personal data within that database may be used. A case in point was in 2018 when Google reportedly bought Mastercard credit card data in the US to help it track users’ offline spending in stores.^[3] One of the concerns that arose from privacy rights groups is whether consumers will be compensated from Mastercard’s financial gain under the sale.

It is important to note that access to data does not equate ownership of data. Use and exploitation of purchased data is still subject to the restrictions the seller of the data is subject to, including profiling and automated decision-making restrictions. Such restrictions on data use may be contained in ownership and confidentiality provisions. The legal analysis should therefore identify each relevant layer of rights: rights in the database or compilation, rights to access and use the underlying data, confidentiality obligations, data-protection requirements and any sector-specific restrictions. The resulting position is usually a bundle of limited rights rather than absolute ownership.

^[2] Copyright Act 2022, sections 2(2), 2(5), 3(a) and 108.

^[3] Google and Mastercard in credit card data deal. (2018, August 31). BBC News. <https://www.bbc.com/news/technology-45368040>

Purpose, Lawful Basis and the Limits of Consent

Data monetisation involving personal data constitutes processing under the NDPA. The principles in section 24 therefore apply throughout the commercial lifecycle of the data. Personal data must be processed fairly, lawfully and transparently; collected for specified and legitimate purposes; limited to what is necessary; kept accurate and secure; and retained only for as long as required. Controllers and processors also owe a duty of care and must be able to demonstrate accountability.

Purpose limitation is particularly important where data was originally collected to provide a product or service and is later considered for a separate commercial use. The NDPA requires the compatibility of further processing to be assessed by reference to the relationship between the original and proposed purposes, the nature of the data, the manner in which it was collected, the possible consequences for the data subject and the safeguards available.

It is therefore not sufficient to conclude that a business may monetise data because it lawfully collected it. The proposed use must either be compatible with the original purpose or supported by an appropriate lawful basis.

Section 25 of the NDPA recognises consent, contractual necessity, compliance with a legal obligation, vital interests, public interest and legitimate interests as lawful bases for processing. Where legitimate interests are relied upon, those interests must not override the rights, freedoms and interests of the data subject. The processing must also be within the data subject's reasonable expectations.

A general privacy notice or broad acceptance of terms is inadequate to support every future commercial use.

Where monetisation was not contemplated at the point of collection, the business should determine whether the new purpose is compatible, whether another lawful basis applies or whether fresh consent is required.



Consent should not be treated as a universal solution. Under section 26, the controller bears the burden of proving that consent was obtained. Silence or inactivity does not amount to consent, and consent must be capable of being withdrawn. Whether consent was freely given may also be questioned where access to a service is made conditional on processing that is not necessary for the performance of the contract.

A general privacy notice or broad acceptance of terms is inadequate to support every future commercial use. Where monetisation was not contemplated at the point of collection, the business should determine whether the new purpose is compatible, whether another lawful basis applies or whether fresh consent is required.

Transparency must follow the actual commercial arrangement. Section 27 requires data subjects to be informed of the purpose and lawful basis of processing, the recipients or categories of recipients, the retention period, relevant rights and the existence and consequences of automated decision-making.

Privacy notices should therefore reflect the substance of the proposed use and not merely describe processing in broad terms such as “analytics” or “business improvement”.

Data Provenance and Rights Clearance

The commercial value of a dataset depends on whether the business can establish its source and the rights attached to it. Data provenance is therefore both a technical and a legal issue.

A business should be able to identify where the data originated, how it was collected, the terms communicated at the time of collection and every material transformation or transfer that followed. Where information was obtained from a vendor, platform, public source or commercial partner, the applicable terms should be reviewed to determine whether they permit extraction, analysis, onward disclosure and the intended commercial use.

Public availability should not be confused with unrestricted use. A publicly accessible source may contain copyright-protected material, confidential information disclosed without authority, personal data or information subject to contractual restrictions. Similarly, purchasing access to a dataset does not cure defects in the way it was collected or give the purchaser broader rights than the supplier was entitled to grant.

Rights clearance should extend beyond the source data to the products created from it. The business should determine who may own or use analytical outputs, scores, reports, enriched datasets, synthetic data and models. It should also consider whether those outputs reproduce protected or confidential elements of the source data or allow individuals to be identified.

A data asset register can support this exercise by recording the source, contents, sensitivity, lawful basis, applicable contracts, permitted uses, retention period, access controls and responsible business owner for each material dataset. Until that information is reasonably clear, the data should not be treated as a market-ready asset.



A general privacy notice is inadequate to support every future commercial use. Where monetisation was not contemplated at the point of collection, the business should determine whether the new purpose is compatible, whether another lawful basis applies or whether fresh consent is required.



Building Risk Management into Product Design

The principal risks in data monetisation should be addressed when the product is designed rather than after commercial terms have been agreed. Data minimisation is the starting point. A product may deliver insights without names, account numbers, locations or transaction records. Aggregation and controlled access can reduce exposure without undermining value.

Anonymisation requires care. Removing direct identifiers may only pseudonymise data, which remains personal if people can be identified by combining it with reasonably available information. This is especially relevant to financial, location, behavioural or health data. Anonymisation should be tested against re-identification scenarios and reviewed as technology evolves.

Data quality presents another risk. Inaccurate or outdated information can produce defective analytics, unfair scores and unreliable automated decisions. Accuracy and fairness requirements should inform validation, correction and model testing. Section 37 gives individuals the right not to be subject to solely automated decisions with legal or similarly significant effects, subject to limited exceptions and safeguards including human intervention and a right to contest the decision.

Security measures should reflect the sensitivity, volume and movement of the data. Controls include restricted access, encryption, monitoring, breach-response procedures and limits on onward disclosure. Under Section 40 of the NDPA, a controller must notify the Nigeria Data Protection Commission within 72 hours of becoming aware of a breach likely to create a risk to individuals. A high-risk breach may also require immediate notice to affected data subjects. Using vendors or commercial partners does not remove these obligations. Section 29 requires appropriate technical and organisational measures and a written agreement where a controller engages a processor. The parties should also establish how corrections, objections, withdrawals and erasure requests will be implemented throughout the recipient chain.

Cross-border arrangements require additional analysis. Sections 41 to 43 restrict transfers from Nigeria unless the recipient benefits from an adequate protective framework or another statutory transfer basis applies. The transfer basis must be recorded. These rules may apply not only to transfers to foreign customers, but also to overseas access through cloud hosting, support services or AI infrastructure.

Where processing is likely to create a high risk to individual rights and freedoms, section 28 requires a data privacy impact assessment before processing begins. The assessment should consider necessity and proportionality, identify harm and document the safeguards adopted. The NDP Act General Application and Implementation Directive 2025 provides further operational guidance.^[4] These controls should form part of a project-specific risk framework identifying each risk, the responsible person and evidence that the control is working. The framework should be reviewed as the product, customers and data sources change.

[4] Nigeria Data Protection Act—General Application and Implementation Directive 2025. The Directive became effective on 19 September 2025.

Key Contractual Considerations for Data Transactions

The data agreement is the instrument that converts legal permissions into a commercial product. In most cases, the transaction is better structured as a licence, subscription or controlled-access service than as an outright sale of data.

The agreement should first define the subject matter with precision. It should distinguish between the underlying records, the database, the delivery platform and any reports or analytical outputs. The rights granted should specify the permitted purpose, authorised users, territory, duration, access method, exclusivity and any right to sublicense or share the product.

Restrictions should be equally clear. Depending on the transaction, these may include prohibitions on resale, re-identification, unauthorised profiling, competitive replication, use for marketing, combination with other datasets or development of products for third parties. A restriction that is essential to the commercial model should not be left to implication.

The agreement should also address the source and legal status of the data. Appropriate warranties may cover authority to provide the data, compliance with applicable collection requirements and the absence of known restrictions inconsistent with the licence. Those warranties should be calibrated to the supplier's actual knowledge and control; an absolute warranty of accuracy or lawfulness may be unrealistic where data comes from multiple external sources.

Ownership and use of derived materials require express treatment. The parties should distinguish between enhancements to the supplied data, customer-generated analytics, aggregated results, trained models, embeddings, synthetic data and other outputs. An agreement that allocates ownership of "derivatives" without defining the term may create uncertainty about both parties' ability to use independently developed products.

Where personal data is involved, the agreement should reflect the parties' actual roles as controllers, joint controllers or processors. These roles are determined by their functions and decision-making, not simply by the labels used in the contract. The agreement should allocate responsibility for privacy notices, lawful bases, data-subject requests, security, breach reporting, subprocessors and cross-border transfers.

Commercial provisions remain equally important. Data quality standards, update frequency, availability, error-correction processes and service levels should be aligned with the customer's intended use. The contract should also address audit rights, regulatory cooperation, retention, return or deletion on termination, treatment of backups and derived materials, and the survival of restrictions after access ends.

Warranties, indemnities and liability caps may allocate financial exposure between the parties, but they do not displace statutory responsibility. A regulator or affected data subject may still proceed against the party responsible under applicable law, irrespective of the contractual allocation of loss.

Artificial Intelligence and Derived Data

Artificial intelligence introduces distinct licensing and accountability questions. A general right to “use” data may not be broad enough to permit model training, fine-tuning, testing, retrieval-augmented generation, the creation of embeddings or the development of synthetic datasets.

The agreement should state whether the recipient may use the data to develop model weights, improve products supplied to other customers or generate outputs that compete with the supplier’s own products. It should also allocate rights in the trained model and its outputs, address the possibility of confidential or personal information appearing in those outputs and establish appropriate testing for accuracy, bias and security.

Deletion provisions need to reflect technical reality. Deleting source records, removing information from an active training corpus and changing a model already trained on that information are different processes. The parties should agree on what deletion requires, whether retraining or model unlearning is technically feasible, and what may be retained for security, legal or audit purposes.

Where AI is used to make decisions that produce legal or similarly significant effects, the safeguards in section 37 of the NDPA must be considered. High-risk processing may also require a data privacy impact assessment under Section 28. These issues should be resolved during product design rather than treated as standard contractual boilerplate.



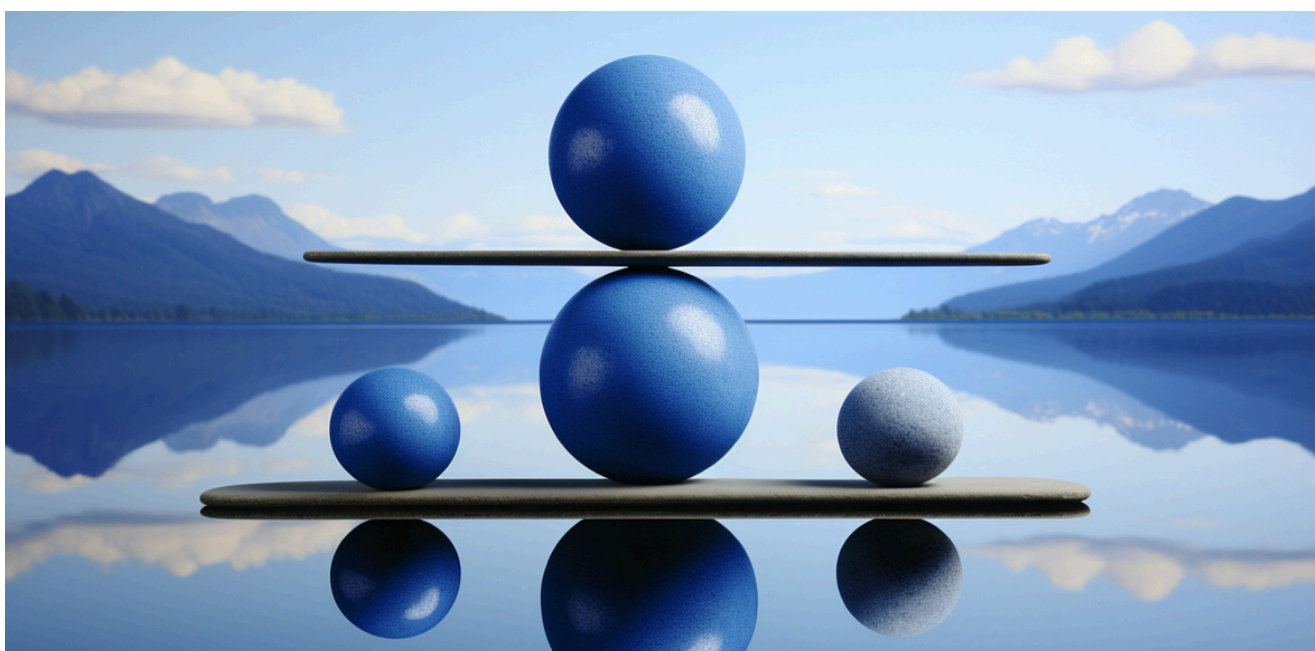
Competition and Consumer Protection Considerations – Finding the Balance

Possessing a dataset is not itself anti-competitive. Concerns arise when its acquisition, combination, withholding or licensing restricts competition or reinforces market power. Section 59 of the FCCPA prohibits agreements whose purpose or actual or likely effect is to prevent, restrict or distort competition. Data-sharing between competitors requires care where it involves information about prices, customers, output, capacity or strategy. Legitimate collaborations should restrict access to competitively sensitive information.

Section 72 prohibits abuse of a dominant position. Depending on the market and dataset, concerns may arise from discriminatory access, unjustified refusals to supply an essential input, tying data access to unrelated products or using exclusivity to deny rivals comparable information. Data concentration may also affect merger review where a transaction combines datasets, raises entry barriers or reduces competition on privacy, quality or innovation.

The competition analysis of a data arrangement is fact-specific. It is about the actual outcome or likely effect of the conduct or arrangement on the market rather than on the conduct itself. Exclusivity may support investment and innovation, while data sharing may improve products or market access. The question is whether a restriction is proportionate to its legitimate commercial objective and whether less restrictive alternatives are available.

Consumer protection is also relevant. Section 123 of the FCCPA prohibits materially false, misleading or deceptive representations in promoting goods and services. Claims about a data-enabled product's privacy, security, accuracy or permitted use should reflect its actual operation. Hidden secondary uses may create consumer-protection exposure in addition to liability under the NDPA.



Governance and Accountability

The commercial owner bears ultimate accountability for the end-to-end data monetization initiative—including commercial performance, compliance, risk posture, and ongoing fitness for purpose. This owner must operate in close alignment with legal, privacy, information security, and technical teams.

Post-launch, the commercial owner must continuously evaluate legal and commercial assumptions. Any material changes—such as updates to data sources, processing purposes, delivery mechanisms, AI integration, or factors altering the lawful basis or risk profile—must trigger a review as rigorous as the pre-launch assessment.

In addition to the above, the commercial owner must also ensure that it conducts a counterparty risk evaluation at different stages of the transactional lifecycle. This is to guarantee that the counterparty does not introduce additional function that alter the lawful basis of the processing or undermine its consent management.

Under the NDPA and GAID, controllers of major importance must appoint a Data Protection Officer (DPO). This role should be meaningfully integrated into team operations rather than treated as a compliance formality. Organizations must also maintain an auditable, living record of data flows, processing purposes, lawful bases, consents, contracts, impact assessments, approvals, risks, and review schedules to enforce joint accountability across commercial, technical, and legal functions.



Concluding Remark

Data monetisation is not simply the sale of information accumulated through a business's platforms, equipment or services. It is the process of converting data into a commercially usable product, whether through internal analytics, market insights, licensing, controlled access or data-enabled services.

It is the development of a commercial product. The value of that product rests on several legal foundations. These include rights in the database or compilation, authority to use the underlying information, compliance with data-protection and sector-specific requirements, and contractual restrictions that preserve control over access, use and onward disclosure.

Depending on the transaction and the market, competition and consumer-protection considerations may also influence how the product is structured and offered. Selecting an appropriate commercial model therefore requires more than assessing revenue potential. A business must consider the source and nature of the data, the purposes for which it may lawfully be used, the persons who will receive it, the method of delivery and the practical ability to enforce restrictions. It must also allocate responsibility for data quality, security, individual rights, regulatory compliance and the treatment of derived products.

Contracts are central to this process, but they cannot replace sound data governance or remove statutory responsibility. A sustainable model depends on clear provenance, reliable data, proportionate controls and continuing oversight as the product, customer base and regulatory environment change.

Good data-monetisation strategies integrate legal analysis into product and commercial design from the outset and this is particularly important for companies building Data-as-a-Service, analytics or AI products. This does more than addressing regulatory exposure. Overall, it improves the quality of the product and places the business in a better position to innovate, offer products that consumers trust, attract investment and scale as technology and regulation evolve.

Authors



Abimbola Ojenike

Partner

E: abimbola@slingstonelaw.com



Oluwadamilola Omotosho

Senior Associate

E: damilola@slingstonelaw.com

Slingstone^{LP}

www.slingstonelaw.com

This publication is for general information only and does not constitute legal, tax or other professional advice on any specific matter or circumstance. While reasonable care has been taken in its preparation, no representation or warranty is made as to its accuracy or completeness. Slingstone LP accepts no liability for any loss arising from reliance on this publication. For questions or advice relating to your specific circumstances, please contact us:

22, Dr. Omon Ebhomenye Street
off Admiralty Way, Lekki I,
Lagos.
Nigeria

Phone : +2348027752339

Email: info@slingstonelaw.com

   @slingstonelaw