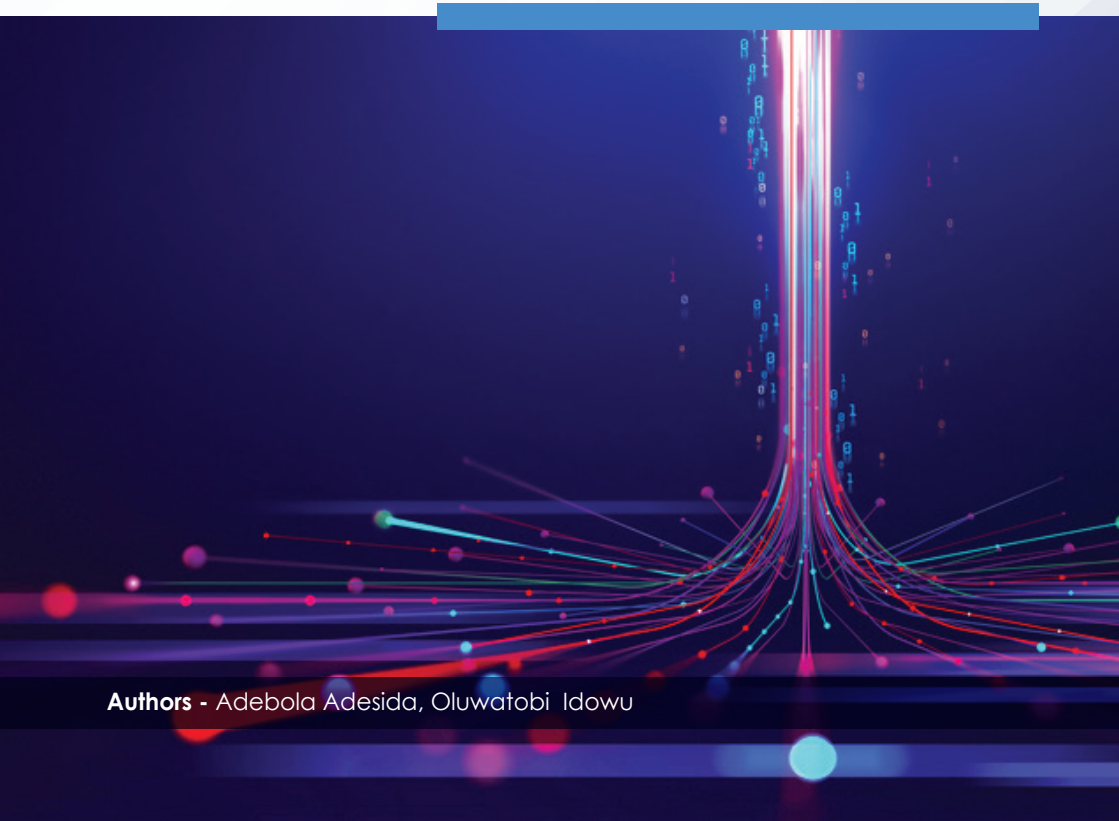
ALP | NG & Co.

Examining the Concept of Joint Data Control Under the Nigeria Data Protection Act



Authors - Adebola Adesida, Oluwatobi Idowu

Introduction

The rise of digital technologies has transformed the way personal data is collected, shared, and utilised. Increasingly, multiple organisations collaborate to process personal data for related purposes. This collaboration raises a critical question under data protection law: who is responsible for ensuring compliance when two or more entities jointly determine the purposes and means of processing?

Joint data control refers to a situation where two or more parties share responsibility for determining the purposes (the "why") and the means (the "how") of personal data processing.[1]

The Nigeria Data Protection Act, 2023 (NDPA or the "Act") and the General Application and Implementation Directive (GAID) 2025 issued by the Nigeria Data Protection Commission (NDPC) regulates the processing of personal data. They recognize the possibility of joint data control and ensure accountability amongst data controllers involved in the collaboration.

While the NDPA does not expressly define or provide for joint data controller, it defines a data controller as an individual, private entity, public commission, agency, or any other body who, alone or jointly with others, determines the purpose and means of processing personal data.[2]

1. Kemal Altuğ Özgün and Iskin Idil Kunt, 'Joint Data Controllership: A Comparative Analysis with the Scope of GDPR and KVKK' Available on Joint Data Controllership: A Comparative Analysis within the Scope of GDPR and KVKK - Lexology Accessed 15 August 2025.
2. NDPA, s 65.
3. Zorluoğlu Yılmaz, Ayça, 'Joint Controllership Under the GDPR - Concept, Responsibilities, and Liability', Juridical Tribune – Review of Comparative and International Law 15 (1) (March 2025): 97.
4. ibid.

Joint control of data arises not from contractual titles but from actual influence exercised by each party over data processing. In other words, an entity that participates meaningfully in deciding why or how data is processed cannot escape liability simply because it labels itself as a "processor" or "partner." Similarly, the presence of multiple actors in data processing does not unilaterally give rise to joint controllership. The underlying element is that the multiple actors must jointly determine the purpose and means of one or more processing activities.[3] Such joint decision-making need not occur contemporaneously and the degree of responsibility of each party does not have to be equal.[4]

Practical Examples of Joint Data Control

Joint control manifests in a range of practical instances:

Telecommunications and Fintech Partnerships: Nigerian mobile network operators often partner with fintech companies to offer mobile money or credit services. Both the operator and the fintech determine how customer personal data is used for service delivery, fraud detection, and marketing.

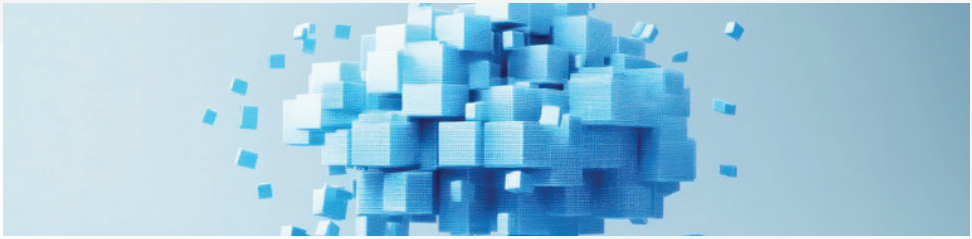
Health Sector Collaborations:
Hospitals may partner with diagnostic laboratories or digital health platforms to manage patient data. If both institutions decide on the scope of data collection and its subsequent use, they jointly control the personal data, even where one has greater technical involvement.

Public-Private Initiatives:
State governments working with private technology providers to deploy utility management systems or other services inevitably share decisions on why and how personal data is processed. This creates joint control in some instances, regardless of whether the public entity regards itself as the primary actor.

Social Media Plug-ins and Advertising:
Following EU jurisprudence, organisations embedding third-party advertising or analytics plug-ins on their websites may become joint controllers with the foreign provider, because both influence the collection and further use of user data.

A notable judicial example is the decision of the Court of Justice of the European Union (CJEU) in Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV.[5] The case involved Fashion ID's use of Facebook's "Like" button on its website, which resulted in automatic transmission of user data to Facebook. The CJEU held that Fashion ID and Facebook were joint controllers because both had an interest in determining the purposes and means of data collection and transmission. This decision underscores that joint control does not require equality of influence but rather a shared determination over essential aspects of processing. Essentially, joint control exists wherever entities collaborate on projects that necessitate shared purposes and decision-making regarding the processing of personal data.

These examples illustrate that joint control is not confined to formal partnerships; it often arises organically from collaboration. Organisations must therefore be alert to the possibility of shared accountability whenever data processing is co-determined.



Legal Obligations of Joint Data Controllers

The NDPA establishes key data-processing principles that bind all data controllers. These obligations equally apply to joint data controllers, as each entity that co-determines the purpose and manner of processing is required to comply with the following principles:

a. Ensuring that personal data is collected and processed in ways that are fair, lawful and transparent.[6] For instance, a hospital and insurer jointly processing patient data must provide clear and consistent explanations to data subjects.
b. Data must be used only for specific, clear, and legitimate purposes known to the data subject.[7] For example, an HR platform and a fintech company that collect data for payroll processing and employee access to salary advance, cannot unilaterally use the same personal data provided to market financial products or other purposes not specifically communicated to the employee upon sign up.
c. Limit the collection of personal data to what is strictly necessary for the stated purpose[8]. For instance, a weather forecast mobile app collecting biometric data just to provide weather updates. This ensures that collaborations do not result in excessive data sharing not required for the purpose of collecting data that could compromise privacy rights.
d. Not retain data for longer than necessary.[9] In joint control arrangements, retention periods must be agreed upon and consistently applied so that one controller does not unduly prolong the storage of personal data.
e. Maintain accurate, complete, not misleading and where necessary, up-to-date records of personal data.[10] Joint controllers must put in place mechanisms for correcting inaccurate information and preventing the use of outdated data in cases where it is necessary for data to be updated.
f. Process personal data in a manner that guarantees appropriate security, including protection against unauthorised access, destruction, or any form of breach.[11] Joint controllers therefore share responsibility for implementing appropriate technical organisational measures to ensure the security, integrity and confidentiality of personal data under their control by implementing encryption, access controls, and secure storage systems.[12]

5. Case C-40/17: Request for a preliminary ruling from the Oberlandesgericht Dusseldorf (Germany) lodged on 26 January 2017.
6. NDPA, s 24 (1)(a) 7. ibid, s 24(1)(b) 8. ibid, s 24(1)(c) 9. ibid, s 24(1)(d) 10. ibid, s 24 (1)(e)
11. ibid, s 24(1)(f) 12. ibid, s 39

Lawful Basis for Joint Data Control

In addition to the above principles, there must be lawful grounds on which the processing of personal data must rest. Section 25 of the NDPA provides for the following grounds:

a. **Consent:** Data subjects may give specific consent to the processing of their personal data. Joint controllers must ensure that consent is validly obtained, not coerced, and may be withdrawn at any time.[13] Consent does not need to be given directly to each joint controller separately; it suffices that one of the parties has obtained consent, provided all joint data controllers are involved in determining why and how the data is processed,[14] and the data subject is clearly informed of the involvement of other parties.[15] This is a common occurrence on the internet. Many websites and applications notify users that their data will be shared with third parties, ensuring transparency in processing data.[16]

b. **Contractual necessity:** Where processing is required for the performance of a contract to which the data subject is a party,[17] joint data controllers are bound to process data strictly for that contractual purpose.

c. **Legal obligation:** Processing may be justified where it is necessary to comply with a statutory or regulatory obligation binding on the controllers.[18] For instance, the Central Bank of Nigeria and commercial banks, in collaboration with the Economic and Financial Crimes Commission.

d. **Vital interests:** Data may be processed to protect the life or health of the data subject or another person.[19] For example, in an emergency healthcare arrangement, hospitals and insurers may jointly process patient data without prior consent.

e. **Public interest or official authority:** Joint control may be justified where the processing is necessary for the performance of a task carried out in the public interest or pursuant to lawful authority.[20]

f. **Legitimate interests:** Controllers may process data where it is necessary for their legitimate interests or those of a third party.[21] However, such interests will not be legitimate if they override the fundamental rights of the data subject; they are incompatible with other lawful grounds for processing data; or the data subject would not have a reasonable expectation that the data will be processed in the manner contemplated.[22]

In joint controllership, both parties must align on the lawful basis being relied upon, as any inconsistency could create compliance lapses and liability risks.

Considerations When Executing a Joint Controller Agreement

As joint controllers share liability and are subject to shared responsibility under the law, it is imperative that they formalise their relationship through an agreement. Such agreements serve not only to allocate responsibilities but also to demonstrate compliance in the event of regulatory scrutiny. Article 26 of the General Data Protection Regulation (GDPR), 2018, which is applicable only in the European Union, underscores this necessity by requiring joint controllers to clearly define their respective responsibilities for compliance, particularly regarding data subject rights.

The following are key considerations when executing a Joint Controller Agreement:

Allocation of Responsibilities:
The agreement must clearly assign which party is responsible for specific obligations vis-à-vis the data subjects,[23] such as providing privacy notices, responding to data subject access requests, or managing breaches. This prevents ambiguity and ensures accountability.

Single Contact Point:
The NDPA requires that a data controller of major importance designate a Data Protection Officer (DPO) to advise the data controller and its employees who carry out data processing activities, to monitor compliance with the Act and the controller's internal policies, and to serve as the point of contact with the NDPC on matters relating to data processing.[24]

In the case of joint controllers, it is recommended that a single DPO or designated contact person be appointed under the agreement to liaise both with data subjects and the NDPC. However, where this is impracticable, the DPOs of each data controller must coordinate closely and operate in alignment on any issues concerning the jointly controlled data or data subjects.

13. NDPA, s 25 (1)(a)
14. Ayça (n 3) 93 -107.
15. NDPA, ss 24 (1)(b); 25 (1)(a)
16. ibid, s 25(1)(a)
17. ibid, s 25(1)(b)(i)
18.ibid, s 25(1)(b)(ii)
19. ibid, s 25(1)(b)(iii)
20. ibid, s 25(1)(b)(iv)
21. ibid, s 25(1)(b)(v)
22. ibid, s 25(2)
23. GDPR, Art. 26(2)
24.NDPA, s 32

Lawful Basis and Retention:
The agreement should specify the lawful basis applicable to each category of processing and define uniform retention periods. It should also provide for secure deletion, anonymization or pseudonymisation[25] once personal data is no longer required.

Data Governance and Dispute Resolution: Joint controllers should establish mechanisms for data governance, including periodic audits, compliance reporting, and structured processes for resolving disputes. This enhances predictability and reduces the risk of conflict.

Termination and Amendment:
The agreement should include clear provisions on how responsibilities will be reallocated in the event of termination or modification of the relationship. This ensures continuity of compliance with data protection obligations as the partnership evolves. Additionally, where a party withdraws from the agreement, the scope of their liability, both prior to and following the withdrawal, must be clearly defined to avoid ambiguity and ensure accountability.

Liability of Joint Data Controllers

Although not expressly indicated under the Act, joint data controllers are at risk of bearing joint liability for any infringement of data protection obligations. The Act recognises joint data control relationships[26] and imposes specific obligations of duty of care and accountability imposed on data controllers[27]. Thus, if at the material time of the breach of the data subject's right, there was a subsisting joint data control relationship, each data controller may be held responsible for the losses and exposed to liability for the infringement.

To mitigate this exposure, agreements between joint controllers could:

a. Provide for indemnities or reimbursement clauses;
b. Define risk allocation mechanisms;
c. Require each data controller to set up and maintain systems that comply with the principles of privacy by design;
d. Ensure that each controller maintains sufficient technical and organisational safeguards to prevent breaches by default; and
e. Introduce reciprocal and periodic compliance confirmation or monitoring measures, including audits.

Ultimately, the law prioritises the protection of data subjects over the existence or absence of contractual arrangements. This is because, even without a Joint Controller Agreement, the Court can still assess the facts and determine the extent of each party's liability.

Enforcement and Compliance

The NDPC is empowered to oversee the implementation of the NDPA,[28] and supervise compliance by data controllers,[29] including those acting jointly. The Commission's powers include investigations, audits, inspections, compliance audits, and corrective measures etc.

Hence, before entering into a Joint Controller Agreement, each party must ensure that its joint data controllers comply with mandatory standards under the Act.

25. ibid, s 39(2)(a)
26. S. 65, which, as stated earlier in this article, defines "data controller" to include a person or entity which jointly with others, determines the purpose and means of processing personal data.
27. S. 24(3)
28. NDPA, s 6(a)
29. ibid, ss 3 and 6

Conclusion

The recognition of joint data control under the NDPA marks a significant step in aligning Nigeria's data protection regime with international best practices. However, it also introduces practical challenges for businesses, public authorities, and service providers.

Organisations need to appreciate that joint data control exists whenever two or more entities jointly determine the purposes and means of processing personal data, regardless of how their relationship is described contractually. All joint controllers share the full spectrum of compliance obligations, including lawfulness, fairness, transparency, security, and accountability. Importantly, liability is joint and several, meaning any controller may be held fully responsible for a breach or violation arising from the joint processing activity. To mitigate these risks, a well-structured Joint Controller Agreement is indispensable, as it clearly allocates roles, responsibilities, and processes for ensuring compliance.

Ultimately, Nigerian organisations involved in collaborative data processing must treat joint control not as a theoretical legal classification but as a practical governance responsibility. It requires deliberate planning, thorough documentation, and sustained accountability. As digital platforms and interconnected services continue to expand, proactive compliance will be essential to the future of digital collaboration in Nigeria.

Authors

Adebola Adesida
Senior Associate
T: +234 201 700 257 0 Ext 114
E: aadesida@alp.company

Oluwatobi Idowu
Associate
E: oidowu@alp.company