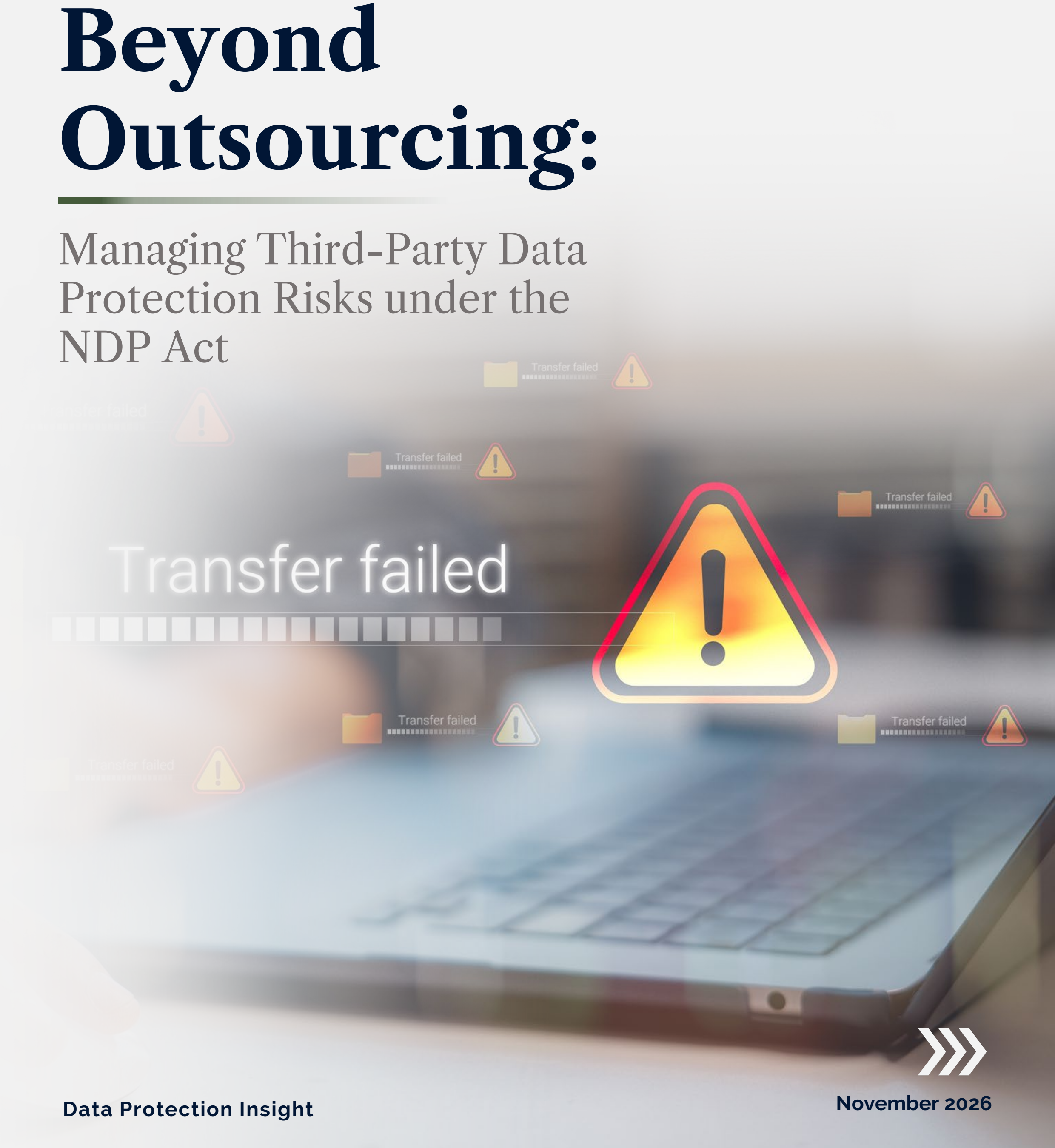
KENNA

Beyond Outsourcing:

Managing Third-Party Data Protection Risks under the NDP Act



Data Protection Insight

November 2026

Introduction

Outsourcing has gradually become a common feature of business operations. Companies engage third parties to support technology, customer management, payment processing, human resources, software services, storage, analytics and other operational functions. When those third parties process personal data on behalf of a company, the arrangement is no longer merely a commercial outsourcing relationship; it also becomes a data protection relationship and, by implication, a data protection concern.

This is significant because privacy is constitutionally protected in Nigeria. *Section 37 of the 1999 Constitution of the Federal Republic of Nigeria* guarantees and protects citizens' privacy, including their homes, correspondence, telephone conversations, and telegraphic communications.[1] *The Nigeria Data Protection Act 2023* (NDP Act) builds on this foundation by providing a legal framework to regulate personal data processing, protect data-subject rights, fulfil controller and processor obligations, and provide recourse where those rights are breached.[2]

For Nigerian businesses, the practical message is clear: outsourcing personal data processing does not remove compliance responsibility. Vendor contracts and Data Processing Agreements must now be reviewed to ensure that they reflect the *NDP Act and the NDP Act-General Application and Implementation Directive 2025* (GAID).

Accordingly, this paper succinctly examines the key contractual and data protection requirements that companies should consider when engaging third-party service providers to process personal data on their behalf. In particular, it considers the essential provisions that should be included in Data Processing Agreements (DPAs), the obligations imposed on data controllers and processors under the Nigeria Data Protection Act 2023 and the General Application and Implementation Directive 2025, and the compliance gaps companies should identify and address when reviewing existing vendor agreements.

01

Constitutional Anchor

Section 37 protects privacy, homes, correspondence and communications.

02

NDP Act 2023

Legal framework for processing, data-subject rights and recourse.

03

GAID 2025

Directive giving practical content to controller and processor duties.

04

Processing Agreements

Written agreements allocating privacy, security and compliance.

Why Vendor Management is crucial under the NDP Act

The NDP Act distinguishes between a data controller and a data processor. A data controller determines the purposes and means of processing personal data, while a data processor processes personal data on behalf of, or at the direction of, a controller or another processor.[3] This distinction matters because many business vendors qualify as processors when they handle personal data for another organisation.

Under the NDP Act, when a controller engages a processor, or a processor engages another processor, the engaging party must ensure the engaged processor complies with the applicable principles and obligations under the Act. The GAID describes this responsibility as "prudent and mandatory".[4] Accordingly, a data processor must comply with the data protection principles and obligations applicable to the data controller, to the extent relevant to its processing activities. The processor must assist with data-subject rights compliance and appropriate technical and organisational measures, provide information reasonably required to demonstrate compliance, and notify the controller or engaging processor when another processor is engaged.[5]

The Act expressly recognises that these measures include a written agreement between the controller and processor, or between processors.[6] This means companies should not rely on general service agreements alone where personal data is being processed. A commercial contract may cover pricing, scope of work, and service delivery, but a Data Processing Agreement should address the privacy, security, accountability, and regulatory issues arising from processing personal data.

ELEMENT I

Data Controller

Determines the purposes and means of processing personal data.

ELEMENT II

Data Processor

Processes personal data on behalf of, or at the direction of, a controller or another processor.

RESULT

Engaging Party Duty

Must ensure the engaged processor complies with the applicable principles and obligations.

What a Data Processing Agreement Should Cover

Article 34 of the General Application and Implementation Directive (GAID) gives practical content to Data Processing Agreements. It provides that, in line with *Section 29(2) of the NDP Act*, a processor is expected to rely on a Data Processing Agreement with the controller in order to process personal data on behalf of that controller.[7]

The GAID provides that a Data Processing Agreement should include the obligations of the controller and processor under section 29 of the NDP Act, the names and addresses of the parties, recitals referring to any principal agreement or service level agreement, the purpose of processing, the location of processing, the scope of processing, lawful bases of processing, responsibilities of the parties, and technical and organisational measures for data protection.[8]

It also requires the Data Processing Agreement to address the outcome of a Data Privacy Impact Assessment where relevant, potential risks, NDP Act compliance, confidentiality, tenure, specific restrictions, indemnity, insurance, force majeure and dispute resolution.[9] The effect is that a Data Processing Agreement should not be treated as a short confidentiality addendum. It should allocate responsibility for privacy, security, compliance evidence, risk controls, and regulatory cooperation.

Named in Article 34

01

Names and Addresses

Names and addresses of the parties, with recitals to the principal agreement.

02

Purpose and Location

The purpose of processing and the location of processing.

03

Scope and Lawful Bases

The scope of processing and the lawful bases of processing.

04

Responsibilities

Obligations of the controller and processor under section 29 of the NDP Act.

05

Technical Measures

Technical and organisational measures for data protection.

06

Indemnity, Insurance

Force majeure, specific restrictions and dispute resolution.

Key Contract Gaps Nigerian Companies Should Watch

Many existing vendor contracts may not have been drafted with the NDP Act and GAID in mind. The first risk is the absence of a clear Data Processing Agreement. If a vendor processes personal data but the contract does not define the processing purpose, scope, location, lawful basis or responsibilities of the parties, the company may struggle to demonstrate that it has properly structured the relationship.

Another common gap is weak security drafting. Under the NDP Act, controllers and processors must implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data. These measures may include de-identification, encryption, resilient processing systems, restoration processes, periodic risk assessments, and regular testing and updating of security measures.[10] Vendor contracts should therefore move beyond broad wording such as "the vendor shall keep information confidential" and require specific, practical security commitments.

It is worth noting that breach response is also critical. Where a breach occurs in relation to personal data stored or processed by a processor, the processor must notify the controller or engaging processor after becoming aware of the breach and respond to information requests required for compliance.

A controller must notify the Commission within 72 hours of becoming aware of a breach which is likely to result in risk to the rights of individuals and must immediately communicate high-risk breaches to affected data subjects.[11] Vendor contracts should therefore include breach notification, cooperation duties, incident information requirements and clear escalation channels.

It is worth noting that Companies should also review sub-processing and cross-border transfer clauses, as the NDP Act requires a data controller or processor that engages another processor to ensure that the engaged processor notifies the controller or engaging processor, as applicable, whenever it appoints a new processor.[12] In addition, personal data must not be transferred from Nigeria to another country unless the recipient is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords adequate protection, or one of the statutory conditions for transfer applies.[13] Where vendors rely on foreign infrastructure or offshore support, the contract should clearly address the basis for transfer and the safeguards relied upon.

The Chapter's Four Subjects

01

No Clear DPA

Purpose, scope, location and lawful basis undefined.

02

Weak Security

Broad confidentiality instead of specific commitments.

03

Breach Response

Notification, cooperation and escalation left unclear.

04

Sub-Processing

Cross-border transfer safeguards left unaddressed.

Why this is a Business Risk

This aspect of data protection concerns, including vendor-related data failures, may create regulatory, financial, criminal and reputational exposure. After investigation, the Commission may issue compliance orders or enforcement orders. An enforcement order may require a controller or processor to remedy a violation, pay compensation to an affected data subject, account for profits realised from the violation, or pay a penalty or remedial fee. The penalty or remedial fee may be up to the greater of ₦10,000,000 or 2% of annual gross revenue in the preceding financial year for a data controller or processor of major importance, and up to the greater of ₦2,000,000 or 2% of annual gross revenue in the preceding financial year for other controllers or processors.[14] In addition to regulatory sanctions, a data controller or data processor may be liable for damages in civil proceedings and, where criminal liability is established, may upon conviction be subject to a fine, imprisonment for a term of up to one year, or both.[15] Where the offender is a company, the principal officers may be also be held culpable.[16]

The GAID also provides that a party to a DPA, other than an individual data subject, must take reasonable measures to ensure that the other party is compliant under the NDP Act. It further provides that every controller or processor shall be accountable for the actions or inactions of third parties it engages or permits to carry out data processing.[17] This makes vendor due diligence a compliance issue, not merely a procurement preference.

EXPOSURE CREATED

- Regulatory sanctions and enforcement orders
- Financial liability — penalties, compensation, account of profits
- Criminal liability for the company and its principal officers
- Reputational exposure from vendor-related data failures

MAJOR IMPORTANCE

₦10,000,000

or 2% of annual gross revenue in the preceding financial year

OTHER CONTROLLERS

₦2,000,000

or 2% of annual gross revenue in the preceding financial year

ON CONVICTION

1 Year

imprisonment, a fine, or both — principal officers may be culpable

Practical Steps for Nigerian Businesses

01 Companies should begin by identifying all vendors that process personal data on their behalf or at their direction. Each relationship should then be reviewed to determine whether there is a written DPA, whether the DPA reflects GAID Article 34, and whether the vendor's role, responsibilities and security obligations are sufficiently clear.

02 Businesses should also update agreements with third-party processors to ensure compliance with the NDP Act.[18] In practical terms, this means reviewing processing purpose, scope, location, lawful basis, security controls, breach notification, sub-processing, cross-border transfer, confidentiality, audit or compliance cooperation, indemnity, insurance, dispute resolution and termination obligations.

03 High-risk vendors should receive closer attention. Where a vendor handles large volumes of personal data, sensitive personal data, critical systems, online platforms, transfers or services that affect data-subject rights, the company should require stronger contractual safeguards and clearer compliance evidence. Particular attention should be given to cross-border processing. The NDP Act requires a data controller or processor to record the basis for each transfer and the adequacy of protection relied upon.[19] Consent is also required before personal data is transferred to a country without an adequacy decision.[20] GAID identifies cross-border data transfer as a circumstance requiring a data protection impact assessment (DPIA).[21]

Conclusion

Vendor management under the NDP Act is no longer only a procurement or contract-management issue. It is now a data protection, compliance and risk-management obligation that requires companies to look beyond the commercial terms of their outsourcing arrangements.

For Nigerian businesses, the priority is not merely to have vendor contracts in place, but to ensure that those contracts properly address how personal data is processed, protected, transferred, retained, returned or deleted. A well-drafted Data Processing Agreement will not, by itself, guarantee compliance. However, it provides an important contractual framework for allocating responsibility, documenting safeguards, managing third-party risk and demonstrating that personal data processing has been structured in line with the NDP Act and GAID.

Companies should therefore revisit their vendor contracts and Data Processing Agreements before a breach, complaint or regulatory inquiry exposes weaknesses in their outsourcing arrangements. In the present regulatory environment, responsible outsourcing requires more than trust in a vendor's capacity to deliver services; it requires verifiable contractual, technical and organisational safeguards for the personal data entrusted to that vendor.

Contributors



Okechukwu Ekweanya

Partner, Data Protection



Muhammad Yasir Abubakar-Sadiq

Associate, Data Protection



Chikaodinaka Monwuba

Associate, Data Protection

Endnotes

1. Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37; Omotayo v Airtel Networks Ltd (2025) LPELR-80342(CA) 20–24; Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission (2021) LPELR-55623(CA) 25–27
2. Nigeria Data Protection Act 2023, s 1(1)(a)–(f)
3. ibid s 65.
4. Nigeria Data Protection Commission, Nigeria Data Protection Act 2023 General Application and Implementation Directive 2025 Sch 7 ('GAID 2025')
5. ibid s 29(1)(a)–(e).
6. ibid s 29(2)
7. Nigeria Data Protection Commission, Nigeria Data Protection Act 2023 General Application and Implementation Directive 2025 art 34(1) ('GAID 2025')
8. ibid art 34(2)(a)–(j)
9. ibid art 34(2)(k)–(t)
10. Nigeria Data Protection Act 2023, s 39(1)–(2)
11. ibid s 40(1)–(4)
12. ibid s 29(1)(e)
13. ibid s 41–43
14. ibid s 48(1)–(5)
15. ibid s 49, s 51
16. ibid s53
17. GAID 2025, art 34(3)
18. ibid art 7(r)
19. Nigeria Data Protection Act 2023, s 41(2)
20. GAID 2025, art 18 (1)(e)
21. ibid art 28(3)(o)



CONTACT

LAGOS
Kenna Place
8, Ogunyemi Road, Palace Way, Oniru PO Box 73002, Victoria Island,
Lagos.

ABUJA
1st Floor, Novare Central,
Plot 502 Dalaba Street,
Wuse Zone 5, FCT 900285,
Abuja.

ENUGU
Michael Place
3, Emmanuel Ngwu Street,
Thinker Corner, 400211
Enugu State.

+234 811 395 1052, +234 811 395 1053 | counsel@kennalp.com | www.kennalp.com