

Data Processing Agreements Under The NDP Act 2023:

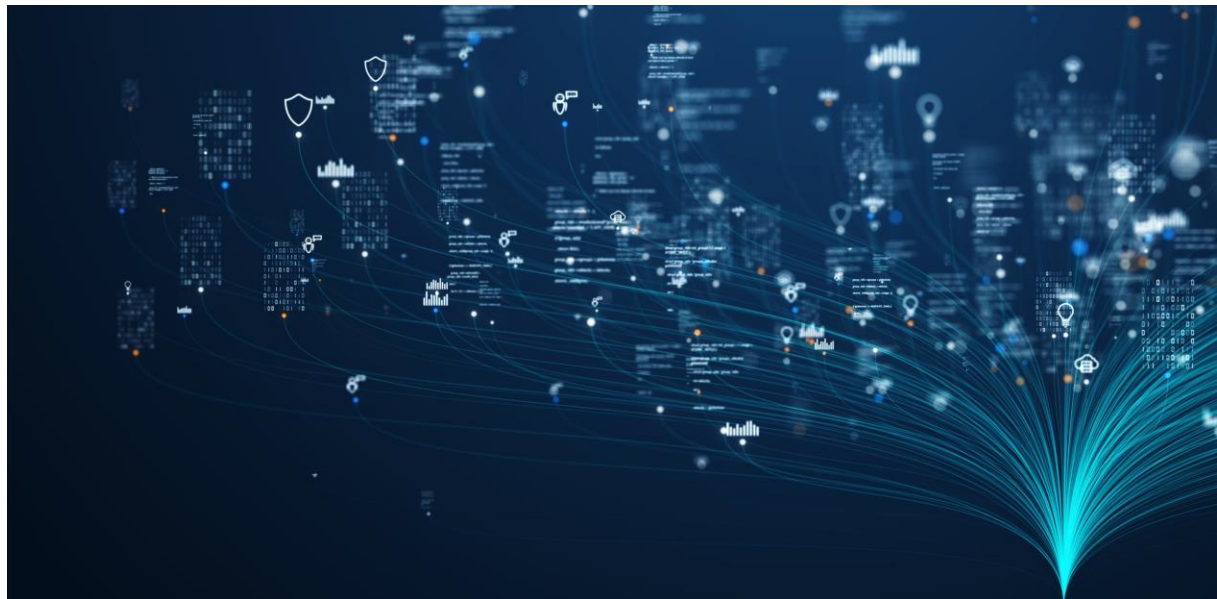
The foundation of trust and lawful
data governance

Introduction

In the modern digital economy, personal data has become a critical commercial asset. Organisations routinely rely on third parties to process personal data, increasing exposure to unlawful processing, data breaches, and regulatory sanctions when roles and safeguards are unclear. The Nigeria Data Protection Act, 2023 (NDP Act), addresses this risk by embedding transparency and accountability at the core of data governance.¹

Central to this framework is the Data Processing Agreement (DPA), a binding instrument that governs the relationship between data controllers and data processors and translates statutory obligations into enforceable contractual duties. Far from a mere formality, the DPA is the foundation of a lawful data processing relationship between a data Controller and a data Processor. In mandating transparency in technical measures and risk assessments, DPAs ensure that data processing is free from prejudice and exploitation. DPAs also serve as a demonstrable commitment to the duty of care, ensuring that personal data is handled professionally to prevent avoidable harm to data subjects.

In light of the foregoing, this article critically examines DPAs under the NDP Act 2023, analysing their legal foundation, mandatory contents, practical importance, and the risks arising from non-execution, while highlighting best practices for effective implementation as a tool for trust-based data governance.



Legal Foundation of Data Processing Agreements in Nigeria

"Under the Nigeria Data Protection Act (NDP Act) 2023, a DPA is a legally binding contract that defines the rules for the sharing, processing, and security of personal data..."

Under the Nigeria Data Protection Act (NDP Act) 2023,² A DPA is a legally binding contract that defines the rules for the sharing, processing, and security of personal data between a data controller and a data processor. This definition under the NDP Act is further reinforced by the NDP Act General Application and Implementation Directive (GAID).³ The GAID sets out the clauses that must be included in a DPA.⁴ and makes the data controller or data processor accountable for the actions or inactions of any third party it engages.⁵ These requirements operate alongside the accountability and security obligations of the data controller under the NDP Act,⁶ and they help position the DPA as the mechanism for implementing these statutory duties.

The primary essence of a DPA is to ensure compliance with the Nigeria Data Protection Act and the GAID 2025, which mandate that a data controller or data processor enter into a written agreement when engaging a third-party processor for data processing activities.⁷ To emphasise the importance of data processing agreements, it must be noted that, in the event of a breach of data privacy rights and the law, specific sanctions are provided under the NDP Act 2023.⁸

Mandatory Contents of a DPA under the GAID 2025

Identification and Recitals

In compliance with these mandatory requirements, every valid DPA must begin with a clear identification of the parties involved. This section should set out the full legal names, registered addresses,⁹ and any relevant corporate identifiers of both the Data Controller and the Data Processor.¹⁰ It should also provide contextual recitals that explain the relationship between the parties, including references to any underlying commercial agreements, such as a Service Level Agreement, Master Services Agreement, or Principal Agreement, under which data processing activities are to be carried out.¹¹

Technical and Organisational Measures

GAID 2025 requires the implementation of appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data.¹³ Where such measures are highly technical or scientific, GAID mandates that they be clearly described in a schedule to the DPA. These measures typically include access controls, authentication protocols, encryption of data in transit and at rest, pseudonymisation where appropriate, secure data storage and transfer, threat detection and response systems, and confidentiality obligations for employees and subcontractors.

Processing Purpose, Scope, and Lawful Basis

Article 34 of GAID requires a DPA to contain a detailed statement of the purpose for which the Processor will handle personal data.¹² The agreement must specify the processing operations to be performed, the categories of data subjects whose data will be processed, and the types of personal data involved, including whether any of the information constitutes sensitive or special-category data. Additionally, the lawful basis for processing must be expressly stated.

Data Protection Impact Assessments and Risk Provisions (DPIA)

The GAID¹⁴ mandates that DPAs must include "the outcome of a DPIA where relevant." The inclusion of DPIA outcomes in DPAs serves several critical functions, including risk identification and mitigation by identifying potential risks to data subjects' rights and freedoms, and accountability, because it creates a documented trail of how risks were assessed and addressed.

Also, the GAID¹⁵ requires DPAs to address "potential risks" associated with data processing. This provision requires parties to identify specific risks to data confidentiality, integrity, and availability; assess the likelihood and severity of risks to data subjects; document mitigation strategies; establish monitoring and review mechanisms; and define responsibilities for risk management.

Mandatory Contents of a DPA under the GAID 2025

Accountability and Compliance Clauses

Article 34(3) of the GAID establishes a critical accountability principle:

"A party to any DPA other than an individual data subject shall take reasonable measures to ensure that the other party is compliant under the NDP Act, accountable to the Commission or, in the case of a foreign party, to a competent regulatory authority outside Nigeria."

This provision creates mutual accountability obligations that go beyond traditional contractual due diligence. It implies that Data controllers must verify that data processors are registered with the NDPC as data controllers or processors of major importance (where applicable), have a designated certified DPO, conduct regular compliance audits, file Compliance Audit Returns (CAR) with the Commission and maintain appropriate technical and organisational measures.

The provision further establishes that "every data controller or data processor shall be accountable for the actions or inactions of third parties it engages or permits to carry out data processing." This creates a chain of accountability that extends throughout the data processing ecosystem, ensuring that data controllers cannot outsource their compliance responsibilities.

Operational and Legal Safeguards

DPAs must establish clear operational rules governing the daily handling of personal data. Among these are the procedures for reporting personal data breaches, which must be communicated to the Controller without undue delay.¹⁶ Additionally, the DPA should address issues relating to business continuity, disaster recovery, confidentiality undertakings, and the legal allocation of liability in the event of non-compliance, regulatory sanctions, or damages arising from data breaches.¹⁷



Key Safeguards List

- **Personal Data Breach Reporting**
- **Business Continuity Planning**
- **Disaster Recovery Procedures**
- **Confidentiality Undertakings**
- **Legal Allocation of Liability**

Legal and Compliance

Consequences of Non-Execution

The failure to execute a valid Data Processing Agreement (DPA) is not a mere procedural error; it goes to the legality of data processing itself under the Nigeria Data Protection Act, 2023 (NDP Act). The consequences of non-execution are both regulatory and commercial, with far-reaching implications for data controllers and processors alike. They include:

- **Administrative Sanctions**

The NDP Act¹⁸ empowers the Nigeria Data Protection Commission (NDPC) to impose administrative sanctions for violations of the Act, including failures to comply with lawful processing and accountability obligations in the event of a data breach or non-compliance with the law. These sanctions may include administrative fines, Compliance orders and Corrective measures.

Importantly, the absence of a DPA significantly weakens an organisation's ability to demonstrate compliance during regulatory investigations or audits. In such circumstances, regulators are more likely to infer negligence or systemic non-compliance.

- **Civil Liability**

Beyond regulatory penalties, failure to execute a DPA increases exposure to civil liability. Where a processor mishandles personal data, affected data subjects may seek compensation for material or non-material damage, particularly when the controller failed to implement appropriate contractual safeguards.

- **Reputational Exposure**

Reputational damage is also a major risk. In today's digital economy, where trust matters, organisations with poor data governance can lose customer confidence, investor trust, and valuable business relationships. This risk becomes even greater when the absence of a Data Processing Agreement is exposed during a dispute or investigation. If the Nigerian Data Protection Commission publicly sanctions such an organisation, the negative attention can quickly damage its reputation and credibility beyond the immediate legal issue.

Conclusion

The NDP Act 2023 represents a decisive shift towards accountability-driven data governance in Nigeria, with the Data Processing Agreement (DPA) positioned as its central compliance mechanism. DPAs are not optional contractual instruments but legal necessities that determine the lawfulness of data processing relationships. As reinforced by the GAID 2025, DPAs operationalise statutory obligations, allocate responsibility across the data processing chain, and mitigate regulatory, civil, and reputational risks. Failure to execute a compliant DPA exposes organisations that process personal data to sanctions, liability, and weakened regulatory defence. Beyond compliance, DPAs foster a culture of trust, risk awareness, and institutional accountability.

It is therefore recommended that, to mitigate these risks and ensure compliance with the NDP Act and GAID, organisations must not only execute DPAs but approach it as living governance instruments rather than static contractual obligations. Conducting robust vendor due diligence using standardised, regulator-aligned templates; scheduling periodic audits and reviews; keeping DPAs updated; and training key personnel, among others, are best practices essential for drafting and implementing Data Processing Agreements.

1. Nigeria Data Protection Act, 2023, Section 24 on Principles of Personal Data Processing
2. Nigeria Data Protection Act, 2023, Section 29(2)
3. General Application and Implementation Directive (GAID) 2025, Article 34(1)
4. Ibid., Article 34(2)
5. Ibid., Article 34(3)
6. NDP Act, Sections 29 and 39
7. NDP Act, Section 29(2)
8. NDP ACT, Sections 48 and 49
9. Ibid, Article 34(2)(b&c)
10. Such as the registered name of the DC/DP and the Incorporation number
11. General Application and Implementation Directive, Article 34(2)(d)
12. General Application and Implementation Directive, Article 34(2)(e)
13. GAID, Article 35 and NDP Act, Section 39
14. Article 34(2)(k), GAID
15. Article 34(2)(l) , GAID
16. Section 40(2) of the NDP Act provides that "a data controller shall, within 72 hours of becoming aware of a breach which is likely to result in a risk to the rights and freedoms of individuals, notify the Commission of the breach and, where feasible, describe the nature of the personal data breach including the categories and approximate numbers of data subjects and personal data records concerned. The Data Controller also has the duty to immediately notify affected data subjects immediately after becoming aware of the breach in order to ensure that data subjects are not unlawfully targeted as a result of the breach
17. GAID, Article 34(2)(o-t)
18. NDP ACT, Sections 48 and 49

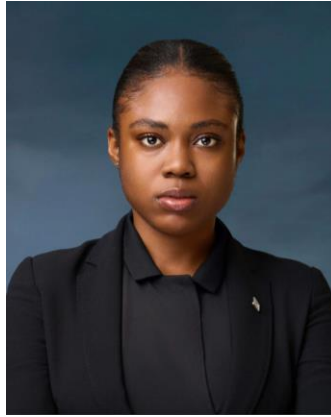
Contributors

12



Nimma Jo-Madugu

Partner, Data Protection



Chidera Mbaogu

Associate, Data Protection



Michael Arinze

Associate, Data Protection



CONTACT US

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