KENNA

Data Protection Impact Assessment as a Strategic Compliance Tool:

What Nigerian Businesses and Corporations Should Know

Data Protection Insight

July 2026

Introduction

With the advent of emerging technologies such as artificial intelligence, Nigeria's data economy continues to expand across financial services, health care, e-commerce, education, employment, hospitality, public services and other technology-enabled business models. As companies collect, analyse and store increasing volumes of personal data relating to data subjects,[1] Data protection can no longer be treated as a back-office compliance issue. The Nigeria Data Protection Act 2023 (NDP Act) recognises this broader economic context by reinforcing the legal foundations of Nigeria's digital economy through the trusted use of personal data.[2] For businesses, this means that compliance now goes beyond publishing privacy notices, cookie policies or obtaining consent; organisations must be able to demonstrate that personal data is processed lawfully, fairly, transparently, securely and accountably.[3]

One important tool for achieving this is the Data Privacy Impact Assessment (DPIA) required under the *NDP Act*. When properly deployed, a DPIA enables an organisation to identify privacy risks before a data-intensive project begins and design safeguards before those risks become regulatory, operational or reputational problems.

This article examines the concept and legal framework of DPIA, and its importance in assessing business risk for organisations that process personal data on a day-to-day basis.

01

Preventive by Design

Identifies privacy risks before a data-intensive project begins.

02

Statutorily Required

Mandated under the NDP Act for high-risk data processing activities.

03

Governance Enabler

Anchors board-level oversight of privacy, IT and vendor risk.

What is a DPIA, and When Does a Business Need One?

A DPIA is a structured, pre-processing risk assessment used to analyse how data processing activities might impact individuals' privacy. It helps organisations identify potential risks, assess their severity, and implement measures to reduce them.[4]

Under the *NDP Act,* a DPIA is required where the processing of personal data is likely to result in a high risk to the rights and freedoms of a data subject by reason of its nature, scope, context and purposes.[5] This means that not every processing activity will require a DPIA. However, where a business intends to process personal data in a way that may significantly affect individuals, a DPIA should be considered at the planning stage.

The Nigeria Data Protection Act 2023 General Application and Implementation Directive ("GAID") 2025 gives further practical guidance. It states that a DPIA is mandatory and must be filed with the Nigeria Data Protection Commission in several circumstances, including profiling, automated decision-making with legal or similarly significant effects, systematic monitoring, processing of sensitive or highly personal data, processing involving vulnerable data subjects, deployment of innovative technological solutions, financial services through digital devices, health care services, e-commerce services, public surveillance cameras, educational services, hospitality services and cross-border data transfers.[6]

For Nigerian businesses, this list is commercially important. A fintech credit-scoring tool, an employer's automated recruitment platform, a hospital's patient-management system, a school's student-record database, an e-commerce profiling tool, a hotel guest-management system or a company's public-facing CCTV system may all raise DPIA issues, depending on the nature and scale of the processing.

Prior Consultation Requirement

The NDP Act requires consultation with the Commission before processing when, despite the proposed measures, the DPIA indicates that the processing would still pose a high risk to the rights and freedoms of data subjects. In high-risk cases, the DPIA becomes part of the organisation's regulatory engagement strategy.

When the Law Requires

The NDP Act sets out the minimum content of a DPIA as follows:

a.

Systematic Description
It must contain a systematic description of the envisaged processing and its purpose, including any legitimate interest pursued by the data controller, data processor or third party;

b.

Necessity & Risk Assessment
It must also assess the necessity and proportionality of the processing, the risks to the rights and freedoms of data subjects, and

c.

Mitigating Measures
the measures proposed to address those risks, including safeguards, security measures and mechanisms for protecting personal data.[7]

These statutory elements are important because they connect the DPIA directly to business decision-making. Before launching a data-driven product or process, management should be able to answer four practical questions: ***What personal data are we processing? Why do we need it? What could go wrong for the individuals affected? What safeguards have we put in place?***

The NDP Act also requires consultation with the Commission before processing when, despite the proposed measures, the DPIA indicates that the processing would still pose a high risk to the rights and freedoms of data subjects.[8] This makes the DPIA more than an internal checklist. In high-risk cases, it may become part of the organisation's regulatory engagement strategy.

The GAID gives the DPIA requirement a stronger technology-governance focus by recognising that new technologies and processing techniques may create unintended adverse consequences for the lives and livelihoods of data subjects.[9] It also requires organisations deploying emerging technologies, such as artificial intelligence, the Internet of Things and blockchain, in the processing of personal data to consider the NDP Act, the GAID and other regulatory instruments issued by the Commission.[10]

> *"The GAID gives DPIA a stronger technology-governance focus — recognising that AI, IoT and blockchain may create unintended adverse consequences for the lives and livelihoods of data subjects."*

Why DPIAs Matter for Business Risk & Corporate Governance

A DPIA is valuable because it turns data protection from a reactive exercise into a preventive tool. Many businesses/ organisations often fall victim to data breaches, leading to privacy failures, because products are launched, vendors are engaged, or databases are built before privacy risks are properly assessed. A DPIA changes that sequence by requiring the business to critically identify and assess potential risks before implementation.

From a corporate governance perspective, board oversight of data protection compliance, including the implementation of DPIAs, is consistent with the Nigerian Code of Corporate Governance 2018 ("The Code"), as the Code expects the Board to establish the company's risk-management framework, monitor its effectiveness, set the company's risk appetite, receive and review risk reports, and exercise oversight over Information Technology governance.[11]

It also expects the committee responsible for risk management to review the company's IT data governance framework to ensure that IT data risks are adequately mitigated, including risks relating to cyber threats and third-party or outsourced IT service providers.[12] In this context, DPIA should not be viewed only as a data protection compliance document. It can also operate as part of the company's wider governance structure for managing legal, technology, vendor and operational risks arising from personal data processing.

The DPIA also helps test the lawful basis for data collection and processing. Under the NDP Act, personal data processing must rest on a lawful basis, including consent, contract, legal obligation, vital interest, public interest or legitimate interest.[13] Where a company relies on legitimate interest, for instance, the Act provides that such interest will not be legitimate where it overrides the rights, freedoms and interests of the data subject, is incompatible with other lawful bases, or where the data subject would not reasonably expect the processing.[14] A DPIA helps the business test these issues before relying on the selected basis.

THE SEQUENCE SHIFT

In addition, DPIAs support transparency. The NDP Act requires data controllers to provide data subjects with information such as the lawful basis and purpose of processing, recipients of the data, retention period, data-subject rights and the existence of automated decision-making, including profiling.[15] A DPIA helps ensure that these disclosures reflect the actual processing activity, rather than a generic privacy notice.

Furthermore, DPIAs strengthen vendor management. Where a data controller engages a processor, the NDP Act requires the controller or engaged processor to ensure that the processor complies with applicable obligations, assists with data-subject rights, implements appropriate security measures, provides information required to demonstrate compliance, and gives notice when another processor is engaged.[16] A DPIA can expose processor-related risks before contracts are signed.

Moreover, DPIAs are particularly important for automated decision-making. The NDP Act gives data subjects the right not to be subject to decisions based solely on automated processing, including profiling, that produce legal or similarly significant effects. However, this restriction does not apply where the decision is necessary for entering into or performing a contract between the data subject and a data controller, authorised by written law with suitable safeguards for the data subject's rights and interests, or authorised by the data subject's consent.[17] Where automated decision-making is permitted, the controller must implement suitable safeguards for the data subject's fundamental rights, freedoms and interests, including the rights to obtain human intervention, to express the data subject's point of view, and to contest the decision.[18]

Practical Steps for Implementing DPIAs and Common Pitfalls to Avoid

Businesses should integrate DPIAs into internal approval processes for high-risk projects. At a minimum, the process should identify the processing activity, map the personal data involved, confirm the lawful basis, assess necessity and proportionality, identify affected data subjects, evaluate risks, design safeguards, document decisions, and assign responsibility for implementation.

Where the processing activity has enterprise-wide risk implications, the DPIA findings should also be escalated to the relevant management, risk, compliance or IT governance function for review and implementation.

The safeguards should be practical. The NDP Act requires appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data, taking into account the amount and sensitivity of the data, the likelihood of harm, the extent of processing, the retention period and available technologies.[19] Such measures may include de-identification, encryption, resilience of processing systems, restoration processes, periodic risk assessments, testing and regular updating of controls.[20]

Common mistakes should be avoided, such as conducting a DPIA after processing has already started, treating it as a template exercise disconnected from the actual product, system or vendor arrangement, or leaving it to legal and compliance teams alone. Depending on the project, product or technology, information security, procurement, human resources, management and other relevant teams may also need to contribute.

*Where the processing activity has **enterprise-wide risk implications**, DPIA findings should be escalated to the relevant management, risk, compliance or IT governance function for review and implementation.*

Conclusion

For Nigerian businesses and corporations, a DPIA should not be treated as a mere statutory formality. It is a practical compliance and governance tool for identifying privacy risks early, testing business assumptions, improving product governance and demonstrating accountability.

As personal data becomes ever more central to commercial operations, organisations that effectively embed DPIAs into product development, vendor selection, emerging technology deployment and board-level risk oversight will be better positioned to reduce enforcement exposure, protect customer trust and participate responsibly in Nigeria's digital economy. The practical priority is therefore clear: businesses should treat DPIAs not as a box-ticking exercise or one-off compliance document, but as an integral part of responsible data governance.

THE PRACTICAL PRIORITY

Businesses should treat DPIAs not as a box-ticking exercise or a one-off compliance document, but as an integral part of responsible data governance.

Contributors

Okechukwu Ekweanya, MCIArb
Partner, Data Protection

Jessica Obodo-Elue, ACArb
Associate, Data Protection

Muhammad Yasir Abubakar-Sadiq, AICMC
Associate, Data Protection

For further information on the issues discussed in this article, contact our legal team at counsel@kennalp.com

Endnotes

1. Under the Nigeria Data Protection Act 2023, a "data subject" means an individual to whom personal data relates; Nigeria Data Protection Act 2023, s 65.
2. Nigeria Data Protection Act 2023, s 1(1)(h).
3. ibid s 24(1)–(3).
4. One trust, "Data Protection Impact Assessment (DPIA)" < https://www.onetrust.com/glossary/data-protection-impact-assessment > accessed June 24, 2026.
5. ibid s 28(1).
6. Nigeria Data Protection Act 2023 General Application and Implementation Directive 2025 Art 28(3)(a)–(o) ('GAID 2025').
7. Nigeria Data Protection Act 2023, s 28(4)(a)–(d).
8. ibid s 28(2).
9. GAID 2025, Art 28(2).
10. ibid Art 43(1)
11. Financial Reporting Council of Nigeria, Nigerian Code of Corporate Governance 2018 Principle 1, Recommended Practices 1.9–1.10.
12. ibid Principle 11, Recommended Practice 11.5.6.6.
13. Nigeria Data Protection Act 2023, s 25(1).
14. ibid s 25(2).
15. ibid s 27(1).
16. ibid s 29(1)–(2).
17. ibid s 37(1)–(2).
18. ibid s 37(3).
19. ibid s 39(1).
20. ibid s 39(2).

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