UDO UDOMA &
BELO-OSAGIE

# Navigating the NDPA and the GAID

## Understanding the Requirement for a Data Privacy Impact Assessment.

**Jumoke Lambo**
Managing Partner

**Noble Chinwendu**
Associate

**Michael Bamgbose**
Associate

# 1. Background

**1.1.** The Nigerian data protection landscape is currently experiencing an increase in regulatory enforcement actions by the Nigerian Data Protection Commission (''NDPC''). These actions often take the form of newspaper publications listing companies in specific sectors who are required to provide evidence of compliance, warning letters, enforcement orders, or invitations to attend investigations issued to organisations alleged to have violated the provisions of the Nigeria Data Protection Act, 2023 (NDPA).

**1.2.** A recurring theme in a number of the enforcement cases is a request for organisations to submit Data Privacy Impact Assessments (DPIA) with respect to their products and services that involve data collection and processing.

**1.3.** The NDPA, provides that unless a data controller or a data processor fall within the category of organisations that must carry out a DPIA due to their sector of operation or the nature of the processing to be done, a DPIA is only required where the nature, scope, context, or purpose of a processing activity is likely to pose a high risk to the rights and freedoms of data subjects[1].

**1.4.** In practice, the NDPC requests DPIAs to be submitted even in cases where the data controller or the data processor has assessed the processing activity and concluded that it does not, in their opinion, present a high risk to the rights and freedoms of the data subject within the parameters provided in the NDPA.

**1.5.** Against this backdrop, we recommend that data controllers and/or data processors should expressly and explicitly document the process they utilised in arriving at the conclusion that a DPIA is not required because it will not present a high risk to the rights and freedoms of the data subject for each processing activity. This recommendation will apply only in cases where the organisation does not fall within the sectors or categories of processing that are mandatorily required to conduct a DPIA under the General Application and Implementation Directive (''GAID'') issued on 20 March 2025 and became operative on 19 September 2025. In that case, the requirement to conduct a DPIA is automatic, and no preliminary risk evaluation is needed.

We have provided below an overview of the requirements for conducting a DPIA and highlighted its significance for organisations operating under the NDPA.

# 2. Understanding DPIAs

**2.1.** Under the NDPA, a data controller is mandated to conduct a DPIA where the processing of personal data may likely result in a high risk to the rights and freedoms of a data subject by virtue of the nature, scope, context and purposes of such processing activities.

**2.2.** A DPIA is a process designed to identify the **risks** and **impact** of any envisaged processing of personal data, and it comprises:

i. a description of the envisaged processing and its purpose;
ii. an assessment of the necessity and proportionality of the processing in relation to the purpose of the processing;
iii. an assessment of the risks the processing will pose to a data subject; and
iv. the measures envisaged by the data controller to address the risks identified.[2]

[1] Section 28 NDPA and Article 28 of the General Application and Implementation Directive

[2] section 28(4) of the NDPA

**2.3.** From the above definition, a DPIA, in essence, is a process for evaluating the likelihood that processing personal data may create risks, such as unauthorised access, data loss, or improper data sharing that could harm the rights and freedoms of data subjects. A DPIA also considers the potential impact of these risks, including identity theft, discrimination, financial loss, or reputational damage.

## 3. When is a DPIA Required

**3.1.** Under the NDPA, a DPIA must be carried out before any processing activity that is likely to pose a high risk to the rights and freedoms of data subjects.

**3.2.** This raises two concerns:

i. whether the determination of what constitutes a "likely high risk" is to be made subjectively by the data controller, the NDPC or objectively by reference to legal standards.
ii. what happens if a data controller concludes that the processing activity is not likely to pose a high risk, but the NDPC later requires a DPIA based on its own assessment?

**3.3.** To address these uncertainties, the NDPA empowers the NDPC[3] to broaden the circumstances in which a DPIA must be carried out. Exercising this power, the NDPC, through Article 28(3) of the GAID, has made it mandatory for data controllers to conduct and file a DPIA with the NDPC in any of these circumstances[4].

[3] section 28(3) of the NDPA

[4] i. Evaluation or scoring (profiling);
ii. Automated decision-making with legal or significant effects;
iii. Systematic monitoring;
iv. Processing of sensitive or highly personal data;
v. Processing involving vulnerable data subjects;
vi. Deployment of innovative processes, new technologies, or organisational solutions that may pose significant privacy risks;
vii. Development of software for communication with data subjects;
viii. Financial services involving personal data processed through digital devices;
ix. Health care services;
x. E-commerce services;
xi. Deployment of surveillance cameras in public-accessible areas;
xii. Development and implementation of legal instruments or policies requiring the processing of personal data of the general public;
xiii. Educational services involving the processing of student records;
xiv. Hospitality services; and
xv. Cross-border data transfers.

**3.4.** While the list provides helpful clarity on the circumstances in which the NDPC will require a data controller to conduct a DPIA, it also raises important questions. The first is whether the list merely identifies the categories of processing that, in the opinion of the NDPC, are by their very nature inherently likely to pose a high risk to data subjects. The second is whether, beyond the general "likely high risk" threshold under section 28(1) of the NDPA, these listed activities automatically trigger a mandatory obligation to conduct a DPIA, even in cases where, in practice, the processing presents little or no real risk to the rights and freedoms of data subjects.

**3.5.** Several items on the list, such as profiling, automated decision-making, deployment of innovative or new technologies and systematic monitoring, are clearly processing activities that, by their very nature, are likely to create high risks. However, other items on the list are not specific processing operations but refer to broad categories of services, such as hospitality, education, or e-commerce. Including "services" in the list implies that data controllers operating in these sectors may be compelled to conduct a DPIA across all their processing activities, irrespective of whether the nature, scope or purpose of the processing itself is high-risk.

**3.6.** For instance, an e-commerce business that processes payment data or tracks customer behaviour online may meet the likely high-risk threshold that requires a DPIA to be carried out. However, the exact requirement would also apply to a small hospitality provider or educational institution processing only basic, low-risk personal data such as manually collected names and contact details for administrative purposes. In such scenarios, the mandatory obligation to conduct and file a DPIA would appear to be disproportionate, as the likelihood of harm to data subjects is minimal.

**3.7.** Whichever interpretation prevails, one thing remains certain: if an organisation's processing activities falls within any of the categories set out above, it is under a mandatory obligation to:

i. conduct a DPIA and submit it to the NDPC prior to commencing any data processing[5];
ii. ensure the DPIA was reviewed and executed by a certified and NDPC accredited Data Protection Officer ("DPO")[6]; and
iii. incorporate the DPIA's outcome into the NDPA Compliance Audit Return (CAR)[7]

[5] Article 28(3, 28(9) ) of the GAID
[6] Article 28(4), 28(12) of the GAID
[7] Article 42(5) of the GAID


## 4. What is Considered as being a High Risk to the Rights and Freedoms of a Data Subject?

### 4.1. Definition

**4.1.1.** The NDPA does not provide a clear definition of what constitutes "high risk" in relation to the requirement for a DPIA. However, useful insights can be drawn from:

i. Section 40(7) of the NDPA, which outlines factors for assessing whether a data breach is likely to result in high risk; and

ii. Schedule 4 of the GAID, which introduces structured categories of risk likelihood and harm in the DPIA template.

**4.1.2.** From these two sources, it can be inferred that a processing activity may be considered a "high risk" if it has the potential to significantly undermine the confidentiality, integrity, or availability of personal data or if the impact on a data subject's rights, life, reputation or livelihood could be serious, even if the likelihood of the risk materialising is relatively low.

### 4.2. Insights from Section 40(7) of the NDPA

**4.2.1.** Section 40(7) of the NDPA provides useful guidance in the context of data breach assessments. It provides that in determining whether a breach is likely to result in high risk, the NDPC and data controllers may consider:

i. The effectiveness of technical and organisational safeguards (e.g., encryption, de-identification, access controls).
ii. Any subsequent measures taken by the data controller to mitigate
iii. such risk;
iv. The nature, scope, and sensitivity of the personal data involved.

Generally, these same factors are equally relevant for assessing whether processing activities, not only breaches, are likely to result in high risk to the rights and freedoms of data subjects.

### 4.3. Guidance under the GAID

**4.3.1.** Article 28(2) of the GAID expands the discussion by noting that certain circumstances are inherently more likely to create a high-risk eventuality. For example, large-scale processing, the deployment of new technologies, or the introduction of new processing methods may require a DPIA because they could create unintended and adverse consequences for the lives, livelihoods, or rights of data subjects.


**4.4. Schedule 4 of the GAID**

**4.4.1.** Schedule 4 of the GAID provides a structured framework for risk assessment by classifying risks along two dimensions: likelihood (remote, possible, or probable) and severity of harm (marginal, significant, or grave).

**4.4.2. Assessing the Degree of Risk**

i. Remote risk: Where personal data is already in the public domain, limited to basic identifiers (e.g., name, email, phone number), contains no sensitive information, and is adequately secured.
ii. Possible risk: Where decisive credentials (e.g., PINs, passwords, tokens) are involved or where only extraordinary measures (i.e., beyond standard technology or requiring exceptional public interest directives) could enable access.
iii. Probable risk: Where covert or overt access to personal data is likely, and data can be accessed using commonly available or legally mandated means.

**4.4.3. Assessing the Severity of Harm**

i. Marginal/low harm: Processing excludes sensitive data and poses no threat to life or livelihood.
ii. Significant/moderate harm: Processing involves sensitive data, or the processing may create an avenue through which the data subject may lose some marginal fraction of his or her valuables.
iii. Grave/extreme harm: Processing involves decisive credentials or highly sensitive data and may lead to severe consequences such as loss of life, livelihood, or substantial personal harm.

**4.5.** The GAID suggests that “high risk” should be understood as the intersection of likelihood and severity:

i. Even a probable risk categorisation may be classified as high risk if the potential harm is grave (e.g. loss of life or livelihood).

ii. Conversely, a probable risk categorisation involving only low harm may not cross the high-risk threshold.

Accordingly, a processing activity is likely to result in high risk whenever it could expose data subjects to serious harm by its nature, scope, context, or purpose.

Notably, we should emphasise that the obligation to conduct a DPIA applies whenever the processing of personal data is likely to pose a risk to data subjects. This is the case even if, after


reviewing the nature, scope and purpose of the processing activity and considering the safeguards in place, the risk is ultimately judged to be low, either because the measures are sufficient to prevent the risk from materialising or because the potential negative impact on data subjects is negligible.

## 5. Significance of Conducting a DPIA and Consequences of Non-Compliance

**5.1.** A DPIA is now considered a tool for demonstrating accountability, managing risk, and protecting the rights of data subjects. Conducting and submitting a DPIA to the NDPC signals to the NDPC that a data controller is proactive about identifying risks and processing personal data in good faith.[8] Section 48(6) of the NDPA obliges the NDPC to consider factors such as intent, negligence, mitigation measures, and cooperation when determining sanctions. A well-prepared DPIA demonstrates that the data controller has taken steps to prevent harm, which may reduce the severity of penalties.

**5.2.** Failure, refusal, or negligence in conducting a DPIA can expose an organisation to serious consequences. Article 28(6) of the GAID expressly provides that, in addition to other enforcement actions in the NDPA, non-compliance with DPIA obligations may result in restrictions on all platforms where data subjects interact with the controller or processor to carry out transactions involving personal data. This can disrupt business continuity and erode customer trust.

## 6. Conclusion

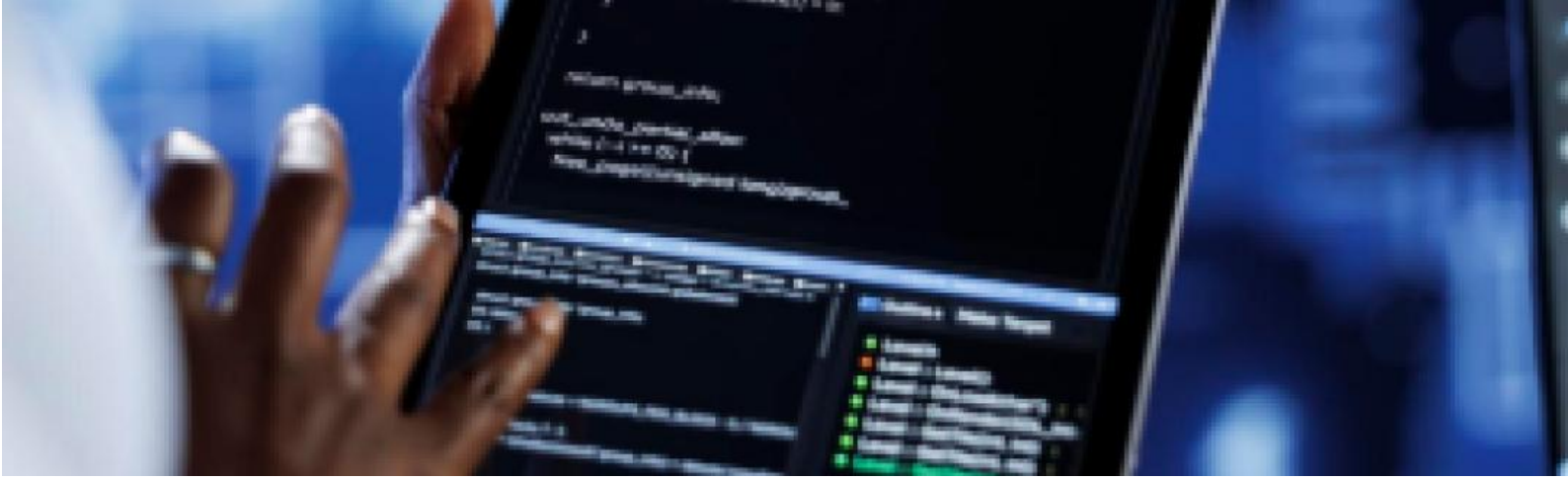
The NDPC's broad interpretation of DPIA requirements may feel heavy handed, especially for low-risk operators. However, this may also reflect the NDPC's push for stronger accountability in Nigeria's data protection landscape.

For organisations, the safest path is to:

i. conduct DPIAs where you fall within the ambit of the law that mandatorily requires a DPIA to be done and approved by the NDPC;
ii. proactively use DPIAs strategically as proof of accountability, not just as a compliance burden; or,
iii. clearly outline the process adopted in arriving at a conclusion that a DPIA is not required for the processing activity.

With the last suggestion above, while the NDPC may still insist on a DPIA, in the event of an investigation or other enforcement action, the documented report will provide proof that the data

[8] Article 48(2) of the GAID



controller or data processor thoroughly analysed the processing activity and the risks that it could pose to the rights and freedoms of data subjects.

It is important to emphasise that while a preliminary determination of whether a DPIA is required constitutes a form of risk evaluation, a DPIA itself is a broader and more comprehensive process. The DPIA not only evaluates potential risks but also examines their likely impact on data subjects, identifies appropriate mitigation measures, and documents the organisation's overall compliance posture. In contrast, the preliminary risk evaluation simply helps an organisation decide whether the proposed processing activity meets the threshold that necessitates conducting a full DPIA.

In all cases, the organisation should document the rationale for its decision whether to conduct or not to conduct a DPIA as part of its accountability obligations and to demonstrate compliance in the event of a review by the NDPC.

***UUBO is a NDPC-licensed Data Protection Compliance Organisation and our data protection practice group is available to address any questions you may have that emanates from this article or any other data protection related matter. Contact the authors at: dpteam@uubo.org or uubo@uubo.org***