

Are You GAID-Ready?

# Essential GAID 2025 Guidelines for DPOs and SMEs



**Gbemisola Adelaja**  
Team Lead, Data Privacy



**Tamaraukuro Brideba**  
Team Lead, Startup Advisory



- **Table of Contents**

**01**

Definition of Acronyms

**02**

Introduction

**03**

Governance and  
Registration

**04**

Core Processing  
Principles and Lawful  
Bases

**05**

Specific Technical and  
Operational Measures

**06**

Transparency and  
Data Subject Rights

# • Definition of Acronyms

Acronym/Term	Full Form
BCR	Binding Corporate Rules
CAR	Compliance Audit Return
CIA	Confidentiality, Integrity, Availability
DCPMI	Data Controller/Processor of Major Importance
DPA	Data Processing Agreement
DPCO	Data Protection Compliance Organisation
DPO	Data Protection Officer
DSVI	Data Subjects' Vulnerability Index
ETs	Emerging Technologies (e.g., AI, IoT, Blockchain)
EHL	Extra-High Level (DCPMI category)
GAID	General Application and Implementation Directive (2025)

Acronym/Term	Full Form
IDPM	Interoperable Data Privacy Measures
ISO 27001	International Standard for Information Security Management System
LIA	Legitimate Interest Assessment
MEM	Monitoring, Evaluation, and Maintenance (Schedules)
NDPA	Nigeria Data Protection Act (2023)
NDPC	Nigeria Data Protection Commission
OHL	Ordinary-High Level (DCPMI category)
SADPR	Semi-Annual Data Protection Report
SCC	Standard Contractual Clauses
SNAG	Standard Notice to Address Grievance
UHL	Ultra-High Level (DCPMI category)

# ● Introduction

Nigeria's new General Application and Implementation Directive (GAID) took effect on 19 September 2025, and they make data privacy stricter and clearer.

If you collect, store, or use personal data for anything and you are not exempted under Section 3 of the Nigerian Data Protection Act 2023 (NDPA), these rules apply to you.

Compliance is not about pleasing the Nigeria Data Protection Commission (NDPC). It is about protecting people's privacy rights. This applies to anyone in Nigeria and Nigerians abroad.

This guide explains the GAID across five areas:

**Governance &  
Registration**

**Core Processing Principles  
and Lawful Bases**

**Specific Technical and  
Operational Measures**

**Transparency & Data  
Subject Rights**

**Ethics &  
Emerging Tech**

# Governance and Registration

(Articles 7 - 13)

## Registration as Data Controller/ Processor of Major Importance (DCPMI)

You must register as a data controller/processor if you fall within the same category:

- 1) Operate in Nigeria
- 2) Processed personal data of 200+ people within six months
- 3) If you are in a high-value sector (finance, health, education, e-commerce, public service, etc.)

A DCPMIs may fall under any of UHL, EHL, or OHL categories, which determine the depth of your obligations.

Articles 7(a), 8, 9

## Filing Compliance Audit Returns (CAR)

If you are categorised as a UHL or EHL, you must:

1. Conduct an NDPA audit within 15 months of starting business
2. File a CAR annually (deadline: March 31)
3. Use a licensed DPCO for the audit

Mustarred is licensed. You may reach out to us on [privacy@mustarred.com](mailto:privacy@mustarred.com) for your CAR.

Articles 7(c),10

## Internal Reporting (Semi-Annual DPO Report)

Your DPO must submit a privacy compliance report to the management every six months. The report should cover areas such as lawful bases, DPIAs, privacy notices, compliance posture, and data subject right management process.

Articles 7(e), 13

## General Compliance Schedule

You must create a documented compliance plan that outlines all your obligations and training timelines.

Think of it as your internal roadmap.

Articles 7(d), 7(g)

# Core Processing Principles and Lawful Bases

(Articles 15, 16, 17, 18, 20, 26)

## Requirements for Consent

Where your lawful basis is consent, you must satisfy the following requirement:

1. Freely given
2. Specific
3. Informed
4. Properly recorded.

In certain instances consent is mandatory including: Direct marketing, sensitive personal data and cross-border transfers without adequacy protection.

**Articles 17, 18**

## Legitimate Interest Assessment (LIA)

You must first carry out an LIA. Your LIA must:

1. Establish necessity,
2. Balance of rights
3. Ensure you are not overreaching, particularly with profiling or targeted ads.

**Article 26, Schedule 8**

## Storage Limitation

Have a clear retention policy. If your business is not regulated, delete or de-identify data within six months after the purpose for collection.

**Article 49(3), Schedule 1(4)**

# • Specific Technical and Operational Measures

(Articles 29, 31, 33, 34)

## • Data Security (MEM Schedules)

You must maintain security schedules (called MEM schedules) that cover staff training, software updates and patching, vulnerability testing and encryption checks. A certified security officer must review them.

Articles 7(f), 29

## • Deployment of Data Processing Software (DPS)

Before launching apps, tools, or tracking software:

1. Conduct a DPIA
2. Apply privacy-by-design
3. Provide a privacy statement before installation

Article 31

## • Measures Against Privacy Breach Abetment

If someone uses your platform to violate privacy and the NDPC alerts you, you must restrict their access immediately.

Article 32

## • Data Processing Agreement (DPA)

If you use a third-party processor:

- sign a DPA
- clearly state purpose, security, storage, and responsibilities
- ensure you follow NDPA, GAID and other relevant privacy laws

You remain responsible for what your processor does.

Article 34

## • Benchmarking IDPMs

You may use global privacy standards for processes like anonymisation or DPIAs.

If the standard requires NDPC approval, get permission first.

Article 35

## • Cross-Border Data Transfer

Using foreign cloud storage counts as a transfer of personal data.

You must:

- transfer only to NDPC-approved “adequate” countries, or
- submit your SCCs/BCRs or Code of Conduct to the NDPC for approval before using them

Article 45, Schedule 5

# Transparency and Data Subject Rights

(Articles 27, 36 - 40)

## Cookie Notices

Your cookie notice must be conspicuously displayed on your website or platform.  
For other types of cookie users must be able to accept or reject.

Articles 7(l), 19

## Data Privacy Impact Assessment (DPIA)

Carry out a DPIA if you are:

- profiling people
- monitoring them
- processing sensitive data
- running fintech or e-commerce operations
- transferring data abroad
  - For activities commence before the GAID became effective, you must carry out DPIAs within **6 months** of GAID's start date on or before March 19, 2026

Article 7(o), 28, Schedule 4

## Grievance Redress and Standard Notice

You must explain how people can complain and remind them they can also report directly to the NDPC.  
When someone sends a SNAG (complaint notice), reply through the NDPC platform.

Articles 7(w), 39, 40

# Transparency and Data Subject Rights

(Articles 27, 36 - 40)

## ● Prioritizing Data Ethics and Dignity

Processing must respect autonomy, privacy, and human dignity. Anything harmful, discriminatory, or degrading is prohibited.

Article 41

## ● Fairness of Intention

Your purpose must be clear and understandable. "Anything not prohibited is allowed" does **not** apply.

Article 42(4)

## ● Organizational Policy on Data Ownership

Recognize that individuals own their data.

Organizations should explore ways data subjects can ethically benefit (e.g., CSR programs).

Article 42(1)

## ● Demonstrable Transparency and Accountability

Be clear about:

- what your technology does
- how your algorithms work (especially profiling)
- expected outcomes
- how people can get help or complain

Article 42(2)

## ● Emerging Technologies (AI, IoT, Blockchain)

Before deploying ETs, conduct a DPIA that considers:

- Algorithmic bias
- Impact on vulnerable groups (DSVI)
- Right to opt out of automated decisions
- Right to be forgotten
- Child and sensitive data safeguards

Article 43

## • Other Things You Should Not Ignore

- Conduct a VAPT at least once a year (ideally every 6 months).
- Begin aligning with ISO 27001 to build a structured, auditable security framework.

Mustarred offers VAPT and ISO 27001 support as well.

## • Conclusion

GAID 2025 requires organizations to integrate privacy into all operations, not as a checkbox exercise but as part of core decision-making. Every process, tool, and partnership that touches personal data must reflect: accountability, transparency, security, and respect for human dignity.

If you need help implementing the GAID, auditing your organization, or conducting DPIAs, reach out to us at **[privacy@mustarred.com](mailto:privacy@mustarred.com)**. Our team of experts is ready to guide you through registration, audits, DPIAs, and all your data privacy needs.

