NEWS UPDATE:

22nd September 2025

Nigeria Data Protection Commission Commences Full Implementation of GAID,[1] 2025.

On March 20th, 2025, the Nigeria Data Protection Commission, exercising its powers under section 61 of the Act, issued the General Application and Implementation Directive (GAID) 2025. The Directive came into effect on September 19th, 2025, following a six-month transition period during which data controllers and processors were expected to align their operations with the GAID's compliance requirements. It is important to note that, with the issuance of the GAID, the Commission has formally ceased to apply the Nigeria Data Protection Regulation (NDPR) 2019 as a regulatory instrument for data privacy and protection. Nonetheless, this development does not invalidate any actions or measures taken under the NDPR prior to the commencement of the GAID.

The newly implemented directives provide detailed guidance and directives for implementing the provisions of the NDPA, clarifying obligations of data controllers and processors. Its commencement is a major development in Nigerian data protection law that will affect corporate obligations, particularly in the handling and processing of personal data of individuals who are within or connected with Nigeria.

Below are some of the most important changes and new requirements under the GAID:

1. **Extent of its Applicability:** The GAID clarifies that the NDPA applies not only to entities domiciled in Nigeria, but also foreign entities that target Nigerian data subjects. It also defines various categories of data subjects who are protected by the NDPA to include: a.) a data subject who is within the territory of Nigeria, regardless of nationality and migration status; (b) a data subject whose personal data has been transferred to Nigeria; (c) a data subject whose personal data is in transit through Nigeria and (d) A Nigerian citizen who is not within Nigeria. In such circumstances, the legal obligation

[1] See, Nigeria Data Protection Act (NDP ACT) General Application and Implementation Directive (GAID) 2025 at <https://ndpc.gov.ng/> accessed on 21st September, 2025.

of a data controller and processor shall be limited to the terms of mutual legal assistance and any applicable International Law.

2. **Mandatory Registration & Audit Requirements:** The Commission classifies data controllers/processors of major importance into 3 levels or categories of major data processing.

   a.) **Ultra-High Level**: GAID describes this category as data controllers/processors of major importance who process personal data of over 5000 data subjects through the means of technology under its technical control or through service contracts.

   b.) **Extra-High Level:** These levels of data controllers/processors of major importance process personal data of over 1000 data subjects through the means of technology under its technical control or through service contracts.

   Data Controller or a Data Processor in the category of UHL or EHL are obligated to register once with the commission and required to file the Compliance Audit Returns (CAR) annually.

   c.) **Ordinary-High Level:** These levels of data controllers/processors of major importance process personal data of over 200 data subjects utilising technology under its technical control or through service contracts. Please note that data controllers or data processors in the category of OHL are obligated to renew their registration with the Commission on an annual basis and are not required to file annual CAR when they renew their registration annually.

   See the GAID 2025[2] for sectors classified as ("DCPMI") and the registration fee for each category. Please be advised that entities designated as Data Controllers/Processors of Major Importance ("DCPMI") are required to conduct NDP Act compliance audit within 15 months of establishment and thereafter on an annual basis.

3. **Requirements for Data Protection Officers (DPOs):** DPOs are expected to compile and submit a semi-annual data protection report to their management. The report submitted must be acknowledged by an officer of the data controller and processor authorised to receive a Record of Processing Activities (RoPA). The RoPA will form part of the company's RoPA. DPCOs are directed to verify the semi-annual report during the NDP Act compliance audit. The GAID also introduces Annual Credential Assessment (ACA) for DPOs. This is to ensure that each DPO maintains the level of

[2] Schedule 7 & 10 of the (NDP Act) General Application and Implementation Directives.

professionalism required to carry out his or her responsibilities towards safeguarding the rights and interests of data subjects. This assessment of DPOs shall be based on the metrics provided in Schedule 3 of the GAID.

4. **Data Subject Rights and Transparency.** The GAID heightens emphasis on making data subject rights easy to exercise. For instance, data subjects have the right to access their data, right of erasure, correction, deletion, and transfer of personal data from one system to another. Privacy notices must be clear and accessible, especially for vulnerable individuals. Privacy policies and notices must be transparent and appropriately provided on platforms/places where data processing is taking place, and cookies/tracking tools require explicit consent.

5. **Adherence to the Lawful Basis for Processing:** The GAID has instructed data controllers and processors to carefully consider and choose the appropriate lawful basis of data processing in order to process personal data.[3] The lawful bases are: a) Consent b) Contractual Obligation c) Legal Obligation d) Vital Interest e) Public Interest, and f) Legitimate Interest.

6. **Complaint Mechanism & Enforcement:** The GAID introduces the use of Data Subject's Standard Notice to Address Grievance (SNAG) for lodging complaints.[4] SNAG will be regarded as a standardised template for demanding internal remediation in an organisation which may be acting in violation of a data subject's privacy. Aggrieved data subjects are encouraged under the GAID to issue a SNAG to a data controller or a data processor where they reasonably believe that the data controller or data processor violated their right to data privacy. NDPC may create an electronic platform through which it might track SNAG.

7. **Data Protection Impact Assessment (DPIA):** GAID makes it mandatory for most organisations to conduct a DPIA.[5] This is required when processing may likely result in high risk to the rights and freedoms of a data subject. For instance, where an entity introduces new technologies or new processing techniques or directives mandating processing of personal data on a large scale. The GAID has directed entities which process such personal data 6 months before the commencement of GAID to conduct a DPIA. Also, entities designated as data controller and processors which deploy software for processing sensitive personal data, among other datasets, are directed to carry out a DPIA and submit same to the Commission within four (4) months after the

---

3 Article 16 of GAID, 2025.
4 Article 40.
5 Article 28.

issuance of this GAID.[6] The DPIA shall be filed with the Commission utilising the template provided in the GAID.[7] A certified DPO duly accredited by the Commission is mandated to vet the completed DPIA and the outcome of a DPIA conducted by a data controller or a data processor shall be part of the NDP Act CAR to be filed with the Commission.

The commission may impose enforcement action on any organization which fails or refuses to conduct a DPIA. It may also place restrictions on all platforms where data subjects may have contact with a data controller or a data processor for the purpose of carrying out any transaction in which personal data is required.

8. **Emerging Technologies**: The GAID mandates data controllers and processors which deploy or intend to deploy Emerging Technologies (ETs)[8] such as Artificial Intelligence, Internet of Things and Blockchain for the purposes of processing personal data to take into consideration: (a) the provisions of the NDP Act, (b) public policy, and (c) GAID, as well as other regulatory instruments issued by the Commission in order to safeguard the privacy of data subjects. The Data Controllers/ Processors that intend to employ ETs for the purposes of processing personal data must set forth technical and organizational parameters in order to design it in compliance with the NDPA. Data Controllers/ Processors who deploy ETs must carry out DPIA on the technologies and the technical and organisational parameters documented and filed with the Commission as part of NDP Act CAR.

9. **New Template for Compliance Audit Returns:** GAID has introduced a new template for audit assessment report. This report, formally known as the data audit questionnaire, is now described as Compliance Audit Returns and it is annexed as one of the schedules in the GAID.[9]

<u>Recommended Steps for Ensuring Compliance and Minimising Risk</u>

To achieve smooth compliance with the NDPA and GAID, and to mitigate potential risks, we recommend that your organisation take the following steps:

1. **Confirm Registration Requirements:** Determine whether your organisation qualifies as a Data Controller or Data Processor of Major Importance and, if so, ensure timely registration with the NDPC.

6 Article 31.
7 Schedule 4.
8 Article 41
9 Schedule 2

2. **Review Existing Data Protection Practices:** Conduct a comprehensive review of your data processing operations, policies, privacy notices, cookie notices, and related documents to ensure full alignment with the Act.

3. **Engage a Licensed DPCO:** Retain a licensed Data Protection Compliance Organisation (DPCO) to audit your company's data protection practices for the preceding year and file the corresponding report with the Commission, especially if this has not yet been done.

4. **Support and verify your DPO's Role:** Follow up with your Data Protection Officer (DPO) to confirm they are compliant with the Act in terms of their role and qualification. Also, confirm that they have prepared and submitted the required semi-annual report to the designated officer of your company. This report will be verified by DPCOs during audits as part of compliance documentation. In addition, ensure that your DPO satisfies the Annual Credential Assessment requirement.

5. **Implement Data Subject Rights Procedures:** Establish clear, documented processes that enable data subjects to exercise their rights to access, correct, delete, or transfer their personal data.

6. **Manage Data Subjects Complaints Effectively:** Put mechanisms in place to acknowledge and address complaints (including Standard Notices to Address Grievances – SNAG) from aggrieved data subjects. Also, ensure that your privacy notices and cookie banners meet the requirements of visibility, consent, and accessibility.

7. **Safeguard Cross-Border Data Transfers:** Ensure that appropriate safeguards are implemented for all cross-border data transfers or data in transit through Nigeria.

8. **Draw up Capacity Building Plan for Staff Members:** Organise regular data protection training for all staff members involved in handling personal data to ensure they understand and can comply with the new obligations under the GAID.

For further information on this News Updates
Please contact John Onyido at
S. P. A. Ajibade & Co., Lagos by
Telephone (+234.8145942221; +234.8118903060),
Fax (+234 1 4605092)
Mobile (+234.8032204371)
Email: jonyido@spaajibade.com
www.spaajibade.com