DUALE, OVIA & ALEX-ADEDIPE

COMPLIANCE MEASURES FOR DATA CONTROLLERS AND PROCESSORS UNDER THE NDPC GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVE (GAID)

#TMTThursdaybyDOA

Telecommunication, Media and Technology (TMT)

doa-law.com

Introduction

In exercise of its powers under Sections 6(c), 61, and 62 of the Nigeria Data Protection Act 2023 (the "Act") to issue regulations, directives, and guidance for achieving the objectives of the Act, the Nigeria Data Protection Commission (the "Commission") on the 20th March 2025 issued the General Application and Implementation Directive (GAID), with an effective date of the 19th September 2025.

The GAID is more than a routine regulatory guideline; rather, it serves as an authoritative guide for interpreting and applying the provisions of the Act, particularly in the context of disruptive technologies and the evolving global landscape of personal data processing. By consolidating and clarifying the obligations of data controllers and data processors, the GAID creates a unified compliance framework for organisations across sectors. Its objective is to ensure that every entity handling personal data in Nigeria does so responsibly, transparently, and in line with global best practices.

In today's #TMTThursday series, we highlighted the key compliance measures under the GAID. These measures apply to both data controllers and data processors, with additional responsibilities for those designated as data controllers or processors of "major importance."

Compliance Measures under the GAID

Under the GAID, data controllers and processors must comply with the following measures to ensure continued adherence to the Act:

1. Register with the Commission as data controllers and processors of major importance (DCPMI) where so designated, in accordance with Section 65 of the Act and the Commission's Guidance Notice on the Registration of Data Controllers and Processors of Major Importance. DCPMIs in the Ultra-High Level (UHL) or Extra-High Level (EHL) categories are required to register once and subsequently file Compliance Audit Returns (CAR) annually, while those in the Ordinary-High Level (OHL) category must renew their registration annually but are not required to file CAR if they do so.

2. Conduct periodic compliance audits within 15 (fifteen) months of commencing business and annually thereafter, to assess and mitigate data processing risks through appropriate technical and organisational measures. DCPMIs in the UHL and EHL categories must file their CAR with the Commission no later than the 31st March of each year.

3. Prepare and maintain semi-annual data protection reports, which provide a detailed analysis of data processing activities within each six-month period.

4. Implement organisation-wide schedules for internal sensitisation and training on data privacy and protection, ensuring personnel are trained within six (6) months of commencement of business operations and annually thereafter, in order to foster a culture of compliance.

5. Designate a Data Protection Officer (DPO), and where necessary, appoint associate DPOs or Privacy Champions to support the DPO, particularly where the organisation processes data or interacts with data subjects across multiple platforms or locations.

6. Publish their organisational privacy policies on their platforms to inform data subjects about data processing activities, their rights, and available complaint mechanisms with the Commission.

7. Provide privacy and cookie notices on the homepage of their websites, allowing data subjects the option to either accept or decline the use of cookies.

8. Conduct Data Privacy Impact Assessments (DPIAs) whenever required under the Act or when directed by the Commission.

9. Notify the Commission of any personal data breach within seventy-two (72) hours of becoming aware of it, and promptly notify affected data subjects if the breach poses a high risk to their privacy.

10. Update agreements with third-party processors to ensure compliance with the Act and alignment with the GAID.

11. Design their systems and processes to make it easy for data subjects to submit data requests and exercise their access rights.

Conclusion

The GAID marks a pivotal development in Nigeria's data protection landscape by providing a comprehensive compliance framework for organisations handling personal data. Its emphasis on registration, audits, reporting, staff training, privacy management, and breach response establishes data protection as a continuous obligation rather than a one-time exercise. With the GAID taking effect on the 19th September 2025, organisations should now focus on sustaining and demonstrating compliance as an integral part of their operations.