Future of Privacy Forum
1350 Eye Street NW
Suite 350
Washington, DC 20005

29 June, 2024

Nigeria Data Protection Commission (NDPC)
12 Dr. Clement Isong
Asokoro, Street 900103,
Federal Capital Territory, Nigeria

To the Chief Executive Officer and all staff concerned,

Comments on the NDPC's proposed General Application and Implementation Directive (GAID)

The Future of Privacy Forum (FPF) is grateful for the opportunity to provide comments on the NDPC's proposed GAID.

About FPF

FPF is a global non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. FPF brings together industry, academics, consumer advocates, and other thought leaders to explore the challenges posed by technological innovation and develop privacy protections, ethical norms, and workable business practices.

FPF's Comments

FPF's comments on the proposed GAID are set out in Annex 1 for your kind consideration.

We welcome the opportunity for future engagement with the NDPC on the proposed GAID. If you have any questions on, or responses to, any of the comments set out below, or if we may be of any further assistance in the development of the proposed GAID, please do not hesitate to contact **Mercy King'ori** (mkingori@fpf.org). Thank you.

Yours sincerely,

Mercy King'ori

Policy Analyst- Africa

Future of Privacy Forum

Annex 1

We thank the Nigeria Data Protection Commission (NDPC) for the opportunity to join other stakeholders in providing feedback on the proposed GAID.

In line with our mission to advance principled data practices in support of emerging technologies, FPF welcomes approaches, policies and tools aimed at promoting the fair, responsible, and trustworthy use of personal data to improve people's lives. These approaches, policies, and tools should also help identify risks and mitigate potential harms, respect legally-recognized rights and freedoms, and provide equitable access to digital technologies.

We therefore welcome the development of the General Application and Implementation Directive by the NDPC. We see the Proposed Directive as a vital step for initiating a holistic and pragmatic conversation on the governance of personal data processing and guiding the responsible development and deployment of technologies in Nigeria in line with the Nigeria Data Protection Act (NDPA) of 2023. We offer the following recommendations to further strengthen the Directive's impact and effectiveness:

1. Clarifying thresholds to be met for certain compliance processes under the GAID;
2. Clarifying conditions to be used to categorize data controllers and processors of major importance;
3. Promoting a balanced approach while considering legal bases of processing personal data;
4. Ensuring provisions on cross-border data flows are in line with the NDPA;
5. Promoting procedural soundness with compliance processes such as the Compliance Audit Returns (CAR);
6. Strengthening the role of the Data Protection Officer (DPO);
7. Ensuring clarity in relation to the private right of action.

We hope that these recommendations will assist the NDPC in the further development of the GAID, and we welcome opportunities for FPF to further contribute to the important endeavor of advancing responsible personal data processing.

1. Clarifying thresholds to be met for certain compliance processes under the GAID

a. Data Protection Impact Assessments:

Article 29(1) of the GAID re-emphasises the need for conducting a data protection impact assessment (DPIA) when personal data processing poses a risk to the rights and freedoms of a data subject, in line with Section 28 of the NDPA. Article 29(3) of the GAID further sets the circumstances and threshold to be met for a DPIA to be conducted, by highlighting specific industries.

We recommend removing the emphasis on industries as the threshold for conducting a DPIA, as such an exercise would inevitably cut across all industries processing personal data, even those not anticipated under the article. Emphasis should rather be placed on the purpose or processing and the risks posed. This eliminates any ambiguity of interpretation that could imply mandatory impact assessments in the aforementioned industries in times where processing does not meet the threshold for conducting a DPIA.

b. Data breach notification procedures:

We welcome the proposal to require data controllers and processors to notify the NDPC in the event of a data breach that would support any remediation efforts. In this respect, we note that the GAID requires controllers and processors to notify a data subject of a data breach immediately.

With respect to this provision, we recommend introducing a threshold to be met for a data breach to be notified to affected data subjects, including the timelines that allow the controller to have collated important information, that is clear and understandable, to share with the data subjects. This will ensure the accuracy of the information shared.

2. Clarifying conditions to be used to categorize data controllers and processors of major importance

We welcome the proposal to impose data processing obligations in an equitable manner by creating different categories of data controllers and processors. In light of this, we commend the provision of Article 8 of the GAID that provides the conditions for designating a data controller and processor of major importance that would be vital to fulfilling their obligations under Section 44 of the NDPA.

Article 8 of the GAID as well as the Guidance Note on designating data controllers and processors of major importance provide a list of factors to be considered in this instance. One of the key considerations is the number of data subjects a data controller or processor is responsible for. Besides that factor, it is not clear how the other factors will be used to classify a data controller or processor of major importance and further into the three sub-groups of data controllers and processors of major importance. This leaves room for ambiguity, consequently affecting any decisions on declassification as a data controller of major importance provided for under Article 9(5) of GAID.

We recommend relying on a risk-based approach towards categorizing data controllers and processors of major importance that will create a predictable system of categorization i.e categorization to be based on the risks associated with their processing activities.

3. Balanced approach while considering legal bases for processing personal data

a. Consent under the GAID

We commend the efforts towards clarifying the application of various legal bases of processing personal data provided for under the NDPA, 2023. In this respect, we note that Article 17(5) of the GAID requires strict scrutiny when other legal bases other than consent are relied upon, indirectly imposing a hierarchy of the legal bases. While considering the limitations of consent in certain circumstances, we recommend placing emphasis on assessing a proposed processing activity to determine the preferred legal basis. On the converse, we believe greater scrutiny should be given on reliance on consent due to the high threshold to be met for valid consent as provided for under Section 26 of the NDPA.

b. Reliance on contract as a legal basis and arbitration

We note that Article 21(5) of GAID mandates that a decision arising from an arbitration process under Article 21(4) be subject to review by the NDPC. Where the parties to an arbitration process have chosen the laws of Nigeria to apply to the arbitration process, this could contradict the Nigerian Arbitration and Mediation Act, 2023 that provides for a review of arbitral awards by an Award Review Tribunal. We recommend rephrasing this provision to align with the country's legislation on arbitration and international best practice.

c. Legitimate interests

Article 27 of the GAID requires that legitimate interest be compatible with other lawful bases of processing such as contract or legal obligation effectively rendering its application as a lawful basis void. Considering the law recognizes legitimate interests as a separate legal basis, this lawful basis must have its own utility and usefulness independently from any other lawful ground. We recommend clearly separating these legal bases by providing examples of situations where reliance of legitimate interest is permitted under the law.

4. Ensuring provisions on cross-border data flows are in line with the NDPA

Article 18(1) of the GAID requires consent to be obtained for personal data being transferred to a country not in the whitelist of countries published by the NDPC. This contradicts Section 43 of the NDPA that provides other bases for transferring personal data out of Nigeria in the absence of any adequacy decision. It does so by placing emphasis on consent as the only legal basis for transferring personal data in those circumstances. We recommend rephrasing this section to align it with Section 43 of the NDPA, noting that consent is only one of the legal bases that can be relied upon as a legal basis for personal data transfers in the absence of an adequacy decision.

5. Promoting procedural soundness with compliance processes such as the Compliance Audit Returns (CAR)

Article 29(5) of the GAID provides that the outcome of a data protection impact assessment shall be part of the NDPA CAR to be filed with the NDPC. Aligning submission of DPIAs with CAR will conflict with the purpose of each of the compliance documents. Under the NDPA and 2022 Guidance note on filing of data protection compliance audit returns, CARs are submitted after a specified period of time of submission under NDPA and GAID i.e. annually while DPIAs in their nature are conducted on a needs basis and once conducted are required to be submitted to the NDPC for review where an assessment reveals existence of risks that a data controller or processor cannot mitigate. Additionally, requiring DPIAs to be part of CARs would absolve certain data controllers - Major Data Processing Ordinary High Level- who have no obligation to submit CARs. We recommend maintaining the submission of DPIAs separately from CARs.

6. Strengthening the role of the Data Protection Officer (DPO)

The DPO has an essential role for accountability of controllers and processors. Article 13 of the GAID would require DPOs to submit to the management of the controller or processor for whom they perform their tasks a bi-annual report on data protection requirements which has to include a detailed list of elements, according to paragraph 5 of the same article. The report will further be verified by an external auditor (a Data Protection Compliance Organization - DPCO - licensed by the Commission). This disclosure of such a report to the DPCO significantly risks undermining the secrecy and confidentiality of the performance of the DPO's tasks - which are two essential elements for the DPO to effectively perform their role, as recognized also by Article 12(7) of the GAID. The DPO has to have access to the details of processing personal data and must be engaged in all issues which relate to the processing of personal data of the controller or processor, and such access is likely to be undermined by this reporting obligation. Additionally, including such a report in the Register of Processing Activities (ROPA) as currently required by Article 13(3) defeats the purpose of the ROPA, which is to clearly lay essential details about all the processing of personal data undergone by the controller or processor. Compiling a semi-annual report with all the details required would also impinge on the limited time resources a DPO has, especially if the DPO will also perform other tasks for the same controller or processor, as will often be the case with small and medium sized organizations. Therefore, we recommend strengthening the role of the DPO in their relationship with the controller or processor by reconsidering the obligation to compile such a report on a semi-annual basis, that needs to be included in a ROPA and that needs to be shared with an external auditor.

7. Emphasis on the private right of action

a. Complaint to Commission by Data Subject

We commend the Commission for emphasizing the private right of action of a data subject as provided by Section 46 of the Nigerian Data Protection Act. However, it is important to clarify whether the right to lodge a complaint with the Commission exists side by side with the private

right of action to a court of competent jurisdiction by a data subject in order to ensure legal certainty.

b. Pre Action Conference

In the General Application and Implementation Directive, the phrase Pre Action Conference (PAC) is used as a prerequisite to the actual hearing (Article 40 (10)), and at the same time as the actual complaint resolution hearing (Article 40 (13)). We recommend that the term be used appropriately for the purpose of clarity and to avoid ambiguity.

Conclusion

Further refining and expanding the Proposed GAID in these ways would not only advance its beneficial impact, but also lead to greater regulatory clarity and alignment on the responsible processing of personal data in Nigeria. The comprehensive and practical guidelines for organizations under the GAID are poised to usher in a new era of data protection in Nigeria, signifying the country's commitment to safeguarding personal data of Nigerian citizens and residents.