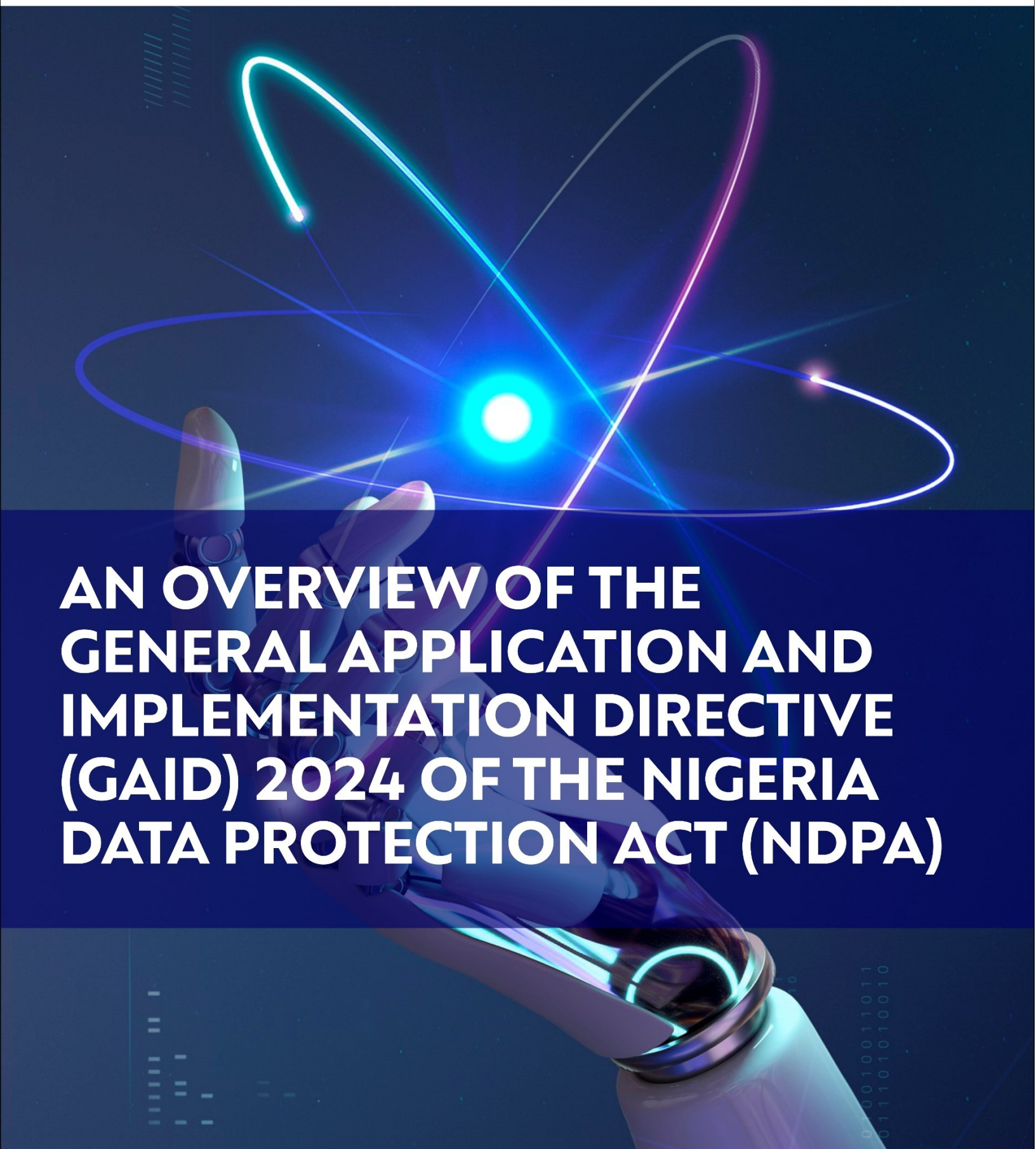
INNO»«CANYON
CONSULTING



AN OVERVIEW OF THE GENERAL APPLICATION AND IMPLEMENTATION DIRECTIVE (GAID) 2024 OF THE NIGERIA DATA PROTECTION ACT (NDPA)

The Nigerian Data Protection Commission (NDPC) recently released a draft implementation directive known as General Application and Implementation Directive (GAID) 2024. Its primary objective is the implementation of the Nigerian Data Protection Act (NDPA), designed to safeguard the right to privacy, in accordance with Nigeria's 1999 constitution (as amended).[1] It provides for guidance in areas of disruptive technologies involving the processing of personal data around the world.[2] While the NDPA is the primary data protection legislation in Nigeria, the GAID seeks to regulate the interpretation and implementation of the provisions of the NDPA. This Article considers the GAID draft policy vis-à-vis the NDPA while highlighting the implications of some of its provisions.

SCOPE AND MATERIAL CONTEXT

Beyond applying to data controllers and data processors domiciled in Nigeria,[3] the NDPA also applies where data controllers or the data processors are neither domiciled, resident, nor operating in Nigeria, but are processing personal data of a data subject in Nigeria.[4] Article 1(2) (c) GAID reiterates this provision by providing that the NDPA applies to a data controller or data processor not domiciled in Nigeria but processing or targeting the personal data of data subjects in Nigeria.

The GAID espouses on the scope of application of the NDPA and significantly introduces a provision which ensures that data controllers and data processors are liable for targeting data subjects within Nigeria even though such controllers are domiciled outside Nigeria. The implication of this is that the NDPA will apply to data controllers resident outside of Nigeria so far as they target Nigerian residents. Put differently, targeting Nigerian residents outside of Nigeria does not exempt controllers or processors from being subject to the NDPA. This laudable provision is a departure from the unrealistic provision of the NDPR which made said law applicable to Nigerian data subjects outside Nigeria.[5]

In respect of the material context of data processing**,** section 24(3) NDPA provides that a data controller or data processor owes a duty of care, in respect of personal data processing and shall promote accountability. A data controller or data processor are to examine the material context of

[1] Section 37, Constitution of the Federal Republic of Nigeria 1999 (as amended).
[2] See preamble of GAID.
[3] Section 2 (2) (a) NDPA.
[4] Section 2 (2) (c) NDPA.
[5] Section 1.2(b) NDPR

data processing and ensure that they conform to the constitutional right to privacy and the objectives set forth in the NDPA.[6] Article 2 (b) GAID further lists the persons, body or authority that owes a duty of care to data subjects. This includes those entities that regulate the matters on the exclusive legislative list which unequivocally signals the application of the NDPA to the federal government.[7] This application to the federal government ensures a broad possibility of data protection rules in Nigeria without limitation. An occurrence which can be for the development of data protection in Nigeria.

REGISTRATION AS A DATA CONTROLLER OR DATA PROCESSOR OF MAJOR IMPORTANCE

Section 44 (1) of the NDPA provides that data controllers and data processors of major importance shall register with the NDPC within six months after the commencement of the Act or on becoming a data controller or data processor of major importance.[8] However, according to Article 9(1) of GAID, a data controller or a data processor of major importance shall register with the NDPC in accordance with the NDPA. GAID further provides that data controllers shall comply with audit requirements stipulated in the NDPA within eighteen months of the commencement of business and thereafter on an annual basis. According to NDPR, organizations must conduct a detailed audit of its privacy and data protection within six months after the date of issuance by the NDPR.[9]

The requirement of registration is not unique to Nigeria.[10] However, one cannot help but wonder the true benefit beyond income generation such a requirement stands to

[6] Article 2 (a) GAID

[7] Under Nigerian law, the matters on the exclusive legislative list are reserved solely for the federal government. Section 4 of the Constitution of the Federal Republic of Nigeria 1999(CFRN) (as amended).

[8] A data controller or processor of major importance is one that keeps or has access to a filing system whether analogue or digital for the processing of personal data. Such data controller or processor of major importance is one that, among other things, processes the personal data of more than two hundred data subjects in six months. For further reading, see Nigeria Data Protection Commission (NDPC), 'Guidance Notice: Registration of Data Controllers and Data Processors of Major Importance' (NDPC/HQ/GN/VOL.02/24)

[9] Section 4.1(5) Nigeria Data Protection Regulation (NDPR). Kindly note that the NDPR remains an extant data protection instrument in Nigeria, though conflicting provisions will be overridden by the NDPA in accordance with Section 63 NDPA.

[10] For further reading on the registration procedure of the UK information commissioner's office, See Information commissioner's office (ICO), https://ico.org.uk/for-organisations/advice-for-small-organisations/whats-new/blogs/data-protection-fee-what-you-need-to-do/#. accessed 30th July 2024.

achieve. This is especially because there are alternative measures through which data protection supervisory authorities can keep track of activities without mandatory registrations.[11] One might even argue that the reliance on this superficial registration and audit requirements places a potential strain on small and medium sized enterprises who will have to incorporate expenses flowing from these audits and registration requirements into their businesses. This practice further creates more hurdles for the ease of doing business in Nigeria.

LEGAL BASIS

The legal basis for processing personal data serves as the justification that authorises the processing of personal data under applicable data protection regulations. Section 25 of the NDPA is in line with Article 16 of GAID provides that it is important for a data controller to carefully assess the lawful basis of data processing before embarking on same. These legal bases which include consent, legal obligation, performance of contract, legitimate interest, etc. are considered subsequently.

i. CONSENT

Consent is one of the legal basis elaborately outlined under the NDPA, with the data controller saddled with the burden of establishing its existence.[12] Silence or inactivity of the data subject shall not constitute consent, it shall be in clear and simple language, accessible format and the data subject shall be informed of the right to withdraw consent prior to them granting it.[13] Lawful data processing that occurred before the withdrawal of consent shall not be affected by a withdrawal of said consent.[14]

Article 17 GAID lists consent as a legal basis which may be used to prioritise the interest of the data subject.[15] According to GAID, consent may be inferred from circumstances which include, a scenario where a data subject's act of participation in a public event and the images taken in that event may be used to report that event – provided that such images shall not be used for profit or commerce-oriented advertisement

[11] Such measures include maintaining a record of processing activities, privacy impact assessments and other general requirements for documentation flowing from the accountability principle enshrined in the NDPA.
[12] Section 26 NDPA.
[13] Section 26(3) NDPA.
[14] A request for consent shall be in clear and simple language and accessible format. Consent shall be in the affirmative, and not based on a pre-selected confirmation and may be provided in writing, orally, or through electronic means. Section 26 (4) NDPA.
[15] Article 17 GAID

without the express consent of the data subject.[16] A data controller in such scenario is required to ensure that images captured do not portray data subjects in a bad light. In addition to other measures of duty of care, a data controller may put participants on notice that images captured may be used for reporting, journalistic or other purposes permitted by the NDPA. At all times where consent is required, a data subject shall be provided with a clear and explicit option to accept or to decline.[17]

The NDPA and GAID both contain interesting provisions on consent that even extends to allusions to scenarios in the latter instrument. This laudable approach marks an improvement on the provisions of the NDPR. However, it would appear that GAID introduces some complications into an otherwise straightforward concept of consent. A good example can be gleaned from the reliance on implied consent under the NDPA and the GAID. Generally, the concept of implied consent within the purview of international data protection law is one that does not receive a positive connotation.[18] This attempt at the white washing of the concept of "implied consent" under the NDPA and the GAID is one that poses significant avoidable confusion for the Nigerian data protection jurisprudence with potential impacts that can potentially slow down trade and other contractual agreements particularly in the EU and other regions where "implied consent" is not permissible. Furthermore, as hypothesized under the GAID, the reliance on constructive or implied consent in circumstances where a data subject has attended a party is nothing short of a strange interpretation of data protection law. Attendance of a party in itself does not constitute an act of consent. It is not unimaginable that a person might attend a party or even a religious event without a desire for their images to be captured. Consenting to attend an event cannot be interpreted as consenting to the capturing and usage of photos. This is just an untenable overreach. Rather than this erroneous attempt at an interpretation and application of data protection law, the NDPC can learn from other jurisdictions such as the EU where alternative and more compliant solutions have since been adopted. Such solutions include the reliance on distinct tags to identify persons who do not consent to

[16] Article 17 (8) GAID
[17] Ibid.
[18] Tom W. Bell, 'The scale of Consent' (2009) PAPER NO. 09-01 <https://ssrn.com/abstract=1322180> . accessed 14th august 2024

pictures or specific sitting arrangements for those who do not wish to be photographed.[19] In regulating data protection law, providing legal definitions ought to suffice. Over regulation to the extent of providing erroneous hypothetical examples bearing this level of detail ought to be avoided. In other words, not all problems can be resolved in legal instruments, some will be resolved in practice as shown with the solution highlighted above.

ii. LEGAL OBLIGATION

The reliance on legal obligation as a legal basis is reflected in Article 25 (1) (b)(ii) of the NDPA. In espousing on this provision, article 23 GAID defines legal obligation as a specific duty imposed by law, or an order of a court of competent jurisdiction, or a responsibility incidental to an obligation imposed by law to carry out an act which requires the processing of personal data.[20] Interestingly, article 23 (2) GAID acknowledges that legal obligations can create derogations from the provisions of the NDPA. More specifically, GAID acknowledges that constitutional derogations from the right to privacy as enshrined in the Nigerian constitution remain lawful derogations to the NDPA.[21] Although this creates a safeguard against arbitrary or unlawful interference in the private lives of data subjects by the government or public authorities, it also calls to question, the blurred lines demarcating the rights to privacy and data protection law (under the Nigerian jurisprudence).

iii. PERFORMANCE OF A CONTRACT

Section 25 (1) (b) (i) NDPA provides that personal data may be processed for the performance of a contract to which the data subject is a party or to take steps at the request of the data subjects prior to entering the contract. In providing more context on this legal basis, Article 21 GAID states that at the preliminary stage of a contract, a data controller may carry out data processing on the data subject for the purpose of due diligence. Where the contract did not materialize, any personal data collected relating to the data subject shall be destroyed within six months unless there is a justifiable ground to archive the data for the purposes of

[19] Justin Reese, 'Effective Photography Opt-out policies for Events' (2016), Leaky Abstractions <https://medium.com/leaky-abstractions/effective-photography-opt-out-policies-for-events-ad58f9dafe71>; Stack-Exchange, <https://photo.stackexchange.com/questions/89665/how-to-handle-photography-permission-in-a-conference> accessed 30th August 2024.

[20] Article 23 (2) GAID.

[21] Section 37 and 45 of the Constitution of the Federal Republic of Nigeria 1999 (CFRN) (as amended).

any future legal claim.[22] A data processing contract shall in addition to the requirement in Section 27 NDPA make provision for its termination prior to the tenure of the contract. Pursuant to Section 46, 1999 Constitution and Section 34(1)(a)(vi) NDPA, a specific term of a contract on personal data processing that ousts or purports to oust the adjudicatory jurisdiction of Nigerian courts or the executive jurisdiction of the Commission shall be treated as void.

One shortcoming of GAID is the attempt to engage in some sort of micro-regulation[23] of issues that would ordinarily be resolved in practice through the requirement of data protection by default and design.[24] Ordinarily, the relevant provision of the NDPA already deemed the processing of data prior to entering the contract as part of the performance of a contract legal basis. Therefore, the provision of GAID that personal data may be processed under this legal basis for the purpose of due diligence is unnecessary and avoidable. The stipulation of a retention period of six months if the contract does not materialise is also unnecessary because there might be more grounds which exceed those listed in the instrument. Under data protection law, the outright stipulation of retention periods (in legal instruments) have proven to be impractical and have even been nullified by the courts for being non-compliant with the retention periods anticipated under relevant laws.[25] In this case, this provision negates the justification for retaining personal data under the NDPA. This means that flowing from section 24 (1) (d) NDPA, personal data ought to be retained for no longer than necessary to achieve the lawful bases for which it was collected. The stipulation of a six month retention period for data processed in scenarios where contracts did not materialise might negate section 24 (1) (d) NDPA because subject to varying circumstances, it might still be necessary to retain the data for longer or shorter than six months. The creation of this unnecessary retention period therefore creates a scenario where data protection compliance is tailored after meeting a set of rules rather than ensuring that compliance

[22] Article 21(2) GAID.

[23] This article uses the term micro-regulation to refer to instances where the law attempts to regulate every possible issue.

[24] See an evidence of such micro-regulation in Article 21 GAID.

[25] In the Tele2sverige case, the court invalidated the EU data retention directive because it listed data retention periods which did not necessarily reflect the necessity of retaining the data. C-203/15 and C-698/15, Tele2 Sverige AB v. Post- och telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others [GC], 21 December 2016, para. 37 and 101.

is achieved on a case-by-case basis. One other concern in this regard is that the GAID does not expressly state that only data necessary for the purpose of the processing ought to be processed. This provision is necessary as it complies with the data minimisation principle thereby ensuring that only the necessary data is processed.[26]

iv. PUBLIC INTEREST

Processing of personal data is also lawful where the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor.[27] GAID provides that the reliance on public interest may be upon a lawful basis of data processing in situations where there is a public health or humanitarian emergency or in the case of a clear and present danger to public safety or if the need arises to address destitution or deprivation for the benefit of the data subject. A data controller should consider the provision of Article 23 GAID when carrying out data processing on the ground of public interest.[28]

There is a potential risk that public interest grounds could be misused or misinterpreted to justify intrusive data processing practices without sufficient safeguards for individuals. This is more so in a country like Nigeria where strong institutions capable of maintaining accountable democratic practices are not at their strongest. Therefore, it is necessary to streamline the language of the law in this regard to reduce abuse. For instance, ambiguous and undefined terms such as "destitution or deprivation" as used under the GAID must be properly defined or avoided.[29]

TRANSFER OF DATA

Section 42 of the NDPA provides that in the absence of adequate protection, a data controller or data processor shall only transfer personal data from Nigeria to another country if, among other things, the data subject has consented to such transfer. Personal data can only be transferred from Nigeria to another country if the data subject has provided and not withdrawn consent to such transfer.[30]

Section 43(2) NDPA further provides that specific international, multi-national cross-border data transfer

[26] Section 24(1)(d) NDPA.
[27] Section 25(1)(b)(iv) NDPA.
[28] Article 23(3) GAID.
[29] Other legal bases referenced in Section 25 NDPA include vital interest, legitimate interest.
[30] Data transfers can also be made subject to defined legal bases such as performance of a contract, vital interests, etc. See section 43 NDPA.

codes, rules or certification mechanisms as transfer mechanisms in Nigeria shall not be adopted without the approval of the national assembly. One interesting concern with this provision is the high level of oversight that is required for the adoption of transfer mechanisms. This poses a shortcoming to the adoption of such transfer mechanisms because of the bureaucracy that is required to obtain the approval of the national assembly.[31] A more efficient approach guaranteeing fast paced privacy regulation would have been the reliance on delegated legislation for such purposes.

Article 46 (2) GAID provides that pending the issuance of guidelines on cross-border data transfer, the explanatory note in Schedule 3 shall be used for the evaluation of countries for the purposes of determining their level of adequacy and for other grounds of cross-border data transfer recognized under the NDPA. The NDPA deviated from the provision of the NDPR which requires the obtaining of an adequacy decision from the attorney general for cross-border data transfers.[32] Instead, the NDPA empowers the NDPC to make decisions on what level of protection is adequate. However, GAID takes it a step further by placing an additional responsibility on the NDPC for the enforcement of fundamental rights and the decisions of courts which seek to advance said rights in such jurisdictions being considered for adequacy of decisions.[33] One can only hope that the NDPC learns from the lessons of the past in the event of its publishing a list of adequate countries.[34]

DATA PROTECTION OFFICER (DPO)

According to the NDPA, a DPO ought to possess expert knowledge about data protection law and practices, including an ability to carry out tasks prescribed under the NDPA and applicable subsidiary legislations.[35] The DPO may be an employee of a data controller or engaged by a service contract, he shall advice the data controller or processor, and their employees and act as the contact point for the NDPC on issues relating

[31] Section 58 of the Constitution of the Federal Republic of Nigeria 1999(CFRN) (as amended).
[32] Cite Article 2.11 NDPR
[33] Article 46 GAID
[34] See Ikigai v National Information Technology Development Agency Suite No. FHC/ABJ/CS/1246/2022 where the court invalidated the adequacy list created by the Defendant because some of the listed countries did not meet the standard of the NDPR. Chukwuyere Izuogu,tech policy, 'data protection law or an independent DPA are prerequisite for a positive adequacy decision in Nigeria: A review of Ikigai v NITDA' https://www.techpolicy.com.ng/category/publications/# accessed 21st August 2024.
[35] Section 32 (1) NDPA

to data processing.[36] Article 12 GAID provides more text on the obligations, duties, and expectations of the role.[37] A data controller of major importance shall designate a DPO with expert knowledge of data protection law and practices, and the ability to carry out the tasks prescribed under this act and subsidiary legislation made under it.

It is clear from the foregoing, that GAID further elaborates on the office of the DPO as provided for in the NDPA. In enforcing the NDPA, GAID provides that a data controller or a data processor shall actively engage its DPO in all issues which relate to the processing of personal data.[38] The effect of having a DPO is crucial to data protection compliance especially because it serves as a mechanism of the accountability principle for ensuring day-to-day compliance. Therefore, capitalizing on the reliance on data protection professionals tasked with helping businesses meet the requirements of the NDPA can help dispense with excessive notification requirements. This will help the supervisory authority focus on a more effective data protection regulation and supervision.

ALTERNATIVE DISPUTE RESOLUTION (ADR)

Though the NDPA is silent on ADR, the NDPR provides a variant of an alternative dispute resolution mechanism through the establishment of the administrative redress panel.[39] It would appear that the reference to ADR under GAID is an attempt to achieve a purpose similar to that sought to be achieved with the administrative redress panel.[40]

Article 21(5) GAID provides that data processing agreements may contain ADR mechanisms which may be reviewed by the NDPC upon a complaint by the data subject or a party to the ADR on varying grounds including fraud, undue influence, etc.[41] ADR is an advantageous

[36] Section 32, NDPA.

[37] Article 12 GAID provides inter alia that the data controller or data processor shall ensure that the DPO does not carry out his or her task under duress, coercion, covert or overt influence. He or she shall not be dismissed or penalized by the data controller or the data processor for performing his or her tasks. The DPO shall directly report to the management level of the controller or the processor.

[38] Article 12 GAID

[39] Article 4.2 Nigeria Data Protection Regulation (NDPR).

[40] The administrative redress panel seeks to resolve data protection-related disputes through administrative orders before the institution of legal actions before a court of competent jurisdiction.

[41] Article 22 (1) GAID.

method of dispute resolution because of its flexibility and less litigious approach which might result in faster resolution of disputes. However, apart from possibly reducing the workload of the NDPC, and in the event of data processing concerns which might imminently and/or irreversibly affect the rights of data subjects, it is otherwise unclear what the advantage of such prompt dispute resolution mechanism might be particularly for the data subject.

A critical defect of reliance on ADR is its substantial costs which impacts the ease of doing business particularly for small and medium sized enterprises, and invariably, the Nigerian economy. One way this mechanism can be well exploited is if the ADR body will be set up internally with the NDPC with little or no cost implication to parties. Anything short of this is just an avoidable expense in a situation where the exercise of the supervisory and enforcement powers of the NDPC would ordinarily have sufficed.

DATA BREACH

According to Section 40(2) the NDPA, data controllers shall, within 72 hours of becoming aware of any breach, notify the NDPC of any possible breach which might result in a risk to the rights and freedoms of individuals. Article 33 GAID states that the data controller shall put in place, appropriate technical and organizational measures to prevent its platform, facility, and network or howsoever called, from being used to breach the privacy of a data subject. It is further provided that when the NDPC notifies a data controller that its platform, facility, network or howsoever called is being used by any person to commit an offence under the NDPA or to carry out a breach of privacy, the data controller shall immediately restrict such person on its platform, facility or network, pending the outcome of an investigation by the NDPC.[42] In determining if a breach of privacy has occurred, the NDPC shall only rely on credible documentary or electronic records.[43] Where a data controller fails, refuses or neglects to carry out the directives of the NDPC to prevent further breach of privacy, the data controller shall be deemed as abetting a breach of privacy and shall be accountable for violation of the NDPA as if it directly committed a breach.[44]

Though an interesting provision, one cannot help but wonder why such complication is being introduced into

[42] Article 33(2) GAID.
[43] Article 33(3) GAID.
[44] Article 33(4) GAID.

the provision for data breaches. This is partly because this issue can effectively be addressed under the provision for the security of processing activities. One might even argue that these provisions are too specific, restrictive, and limiting in relation to the scope of the scenarios in which it might be applicable. For instance, the requirement for controllers to restrict the access of persons who might commit an offence or violate the NDPA underestimates the capabilities of technological advancements in the society. This is because such threat actors might be capable of penetrating a network system in surreptitious ways that merely restricting them might not work. The same can be said about deeming a controller as abetting the NDPC of a breach. A better approach is to stick to the already sufficient requirement for the maintenance of appropriate technical and organisational measures. Such an approach already captures the adoption of adequate security measures which envisage preventing threat actors from gaining access to the system.

DATA SECURITY

Section 39(1) NDPA provides that data controllers and processors shall implement appropriate technical and organizational measures to ensure the security, integrity and confidentiality of personal data in its possession or under its control, including protection against accidental or unlawful destruction, loss, misuse, alteration, unauthorized disclosure, access, etc.

Article 30 GAID provides for monitoring, evaluation and maintenance of data security system, a data controller or processor shall have schedules for monitoring, evaluation and maintenance of data security systems, the schedules shall take into account people, processes and technologies involved in data security and each shall contain applicable technical and organizational measures, a data controller or processor shall assign relevant officers to carry out the tasks under the schedule and stipulate time to take appropriate technical and organizational measures under the schedule which will be vetted by a certified information security officer. A data controller shall carry out the monitoring, evaluation and maintenance of data security systems frequently and shall consider the risks of data processing. Since the concept of technical and organizational measures is ever evolving, it is proposed that the clause “state of the art” should precede the term ‘technical and organizational measures’. This way, the language of the law remains relevant irrespective of advancements in relevant

technical and organisational measures.

INTERNAL AUDIT

Article 7(b) GAID provides that in compliance with the NDPA,[45] audit should be carried out within eighteen months of commencement of business and thereafter on an annual basis. Article 10 GAID further provides that a data controller or data processor of major importance shall file NDPA Compliance Audit Returns (CAR) on an annual basis. In the case of a data controller or a data processor of major importance that was established before the 12th day of June, 2023, it shall file its CAR not later than 31st of March each year.

In relation to similar audit requirements under the NDPR, it has been argued that conducting and filing the statutory audit is fast becoming a tick box exercise and does not equate to compliance.[46] This is usually exemplified by organizations whitewashing their data protection compliance framework using phrases like "NDPR complaint" to boost the public perception of their organization. One cannot help but wonder if these registration requirements will pose a strain to the budget of businesses in Nigeria especially the small and medium enterprises who will likely incur avoidable costs from these audits. These frequent audits might also affect the ease of doing business in Nigeria. It is proposed that small and medium enterprises should be categorized as low revenue organizations for the purpose of audit generation and should all be categorized different from profit making organizations, doing this will certainly help them grow. The small and medium enterprises will therefore be exempted from, or given less auditing requirements. This approach will not harm the compliance of data protection law in the country as the accountability principle which is already in place is enough to achieve the objectives of the auditing requirements, even more effectively.

CONCLUSION

The GAID draft policy introduction has the potential to contribute to a more robust data protection landscape in Nigeria. It also adds harmonization, compliance,

[45] Article 10 GAID.

[46] Ridwan Oloyede,' Data protection compliance:when it becomes a "tick-box Olympics" and a race to nowhere'< https://www.linkedin.com/pulse/data-protection-compliance-when-its-tick-box-olympics-ridwan-oloyede-/?trackingId=JKy%2BiCk4SXuwvtDu5%2FiW9A%3D%3D> accessed 30th of August 2024.

enhanced regulatory framework, accountability, security, innovation, and most importantly, further enforcement measures to the Nigerian data protection space. As identified in this article, the GAID is not without its own shortfalls, and appropriate improvements should be considered where needed.

It is important to acknowledge the fact that GAID cannot capture or resolve all data protection issues in Nigeria. Therefore, the attempt to provide a one-size-fits-all solution to all Nigerian data protection issues should be avoided. Some problems will be resolved in practice once adequate regulatory guidance and framework is provided.