Data Protection in Nigeria – A Review of the Nigeria Data Protection Act 2023

As information technology ('**IT**') expands, the law must also expand to deal with its challenges. Despite its many benefits, the growth of IT has also raised concerns about personal privacy and security, as well as the potential misuse of personal information. On 12th June 2023, President Bola Ahmed Tinubu signed the Nigeria Data Protection Act 2023 (the '**Act**') into law. The Act provides a legal framework for the protection and regulation of personal information and establishes the Nigeria Data Protection Commission ('**NDPC**').

Below are some of the key highlights of the Act:

Objectives and Applicability of the Act

The Act seeks to regulate processing of personal data; ensure that personal data is processed fairly, lawfully and accountably; and to ensure that data controllers and data processors comply with their obligations to data subjects. A '*data controller*' is defined in the Act as an individual, private entity or public body or authority who, alone or jointly with others, determines the purposes and means of processing of personal data; while a '*data processor*' is defined as any individual, private entity, public authority or body who processes personal data on behalf of or at the direction of a data controller or another data processor. A 'data subject' on the other hand is an individual to whom personal data relates.

The Act applies where the data controller or data processor is domiciled, resident or operating in Nigeria; where the processing of personal data occurs within Nigeria and where the data controller and data processor, though not having any presence in Nigeria, processes personal data of data subjects in Nigeria. The Act therefore has some form of extra territorial applicability similar to the Nigeria Data Protection Regulations 2019 ('**NDPR**').

There are however some exemptions to the Act's applicability. For instance, a violation of the Act would not occur when personal data is

processed for personal or household purposes and such processing does not violate the privacy of the data subject. Furthermore, the Act would not apply to the processing of personal data for crime prevention, detection and prosecution, to prevent national public health emergencies, to protect national security, to serve public interest, for educational, journalistic, literary and artistic purposes as well as court and judicial purposes.

However, these exemptions are not blanket as the Act empowers the NDPC to issue legal safeguards on any aspect of data processing exempted from the Act if such processing is likely, in NDPC's opinion to breach Sections 24 (principles of personal data processing) and 25 (lawful basis of personal data processing) of the Act.

Processing of Personal Data

The grounds for processing personal data under the Act are the same under the NDPR. But, the Act introduces another ground which is that personal data may be lawfully processed if it is necessary for '*purposes of the legitimate interests pursued by the data controller or data processor, by a third party to whom the data is disclosed*' provided that the interests do not override the fundamental rights of the data subject, or are incompatible with other lawful basis of processing the data subject's personal data or data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.

Although the Act does not define or clarify what is meant by 'legitimate interests' or how it is to be determined, we think that an appropriate criterion for determining legitimate interest may be an evaluation of the interests of the data subject and those of the data controller and an assessment of which of the interests should take priority.

Data Privacy Impact Assessment

The Act requires data controllers to carry out data privacy impact assessment where the processing of personal data may likely result in high risk to the rights and freedoms of a data subject. If the data protection impact assessment indicates that the processing of the data would result in a high risk to the rights and freedoms of a data subject, then the data controller must notify the NPDC prior to processing the data.

Obligations on Data Controllers and Data Processors

Where a data controller engages the services of a data processor, or a data processor engages the services of another data processor, the data controller or data processor engaging the other must ensure that the engaged data processor complies with the Act; assist the data controller or data processor in the fulfilment of the data controller's obligations to observe the rights of data subjects; put measures in place to ensure the security, integrity, and confidentiality of personal data; provide the data controller or engaging data processor, with information required to comply with the Act; notify the data controller or engaging data processor of the engagement of a new data processor; and have a written agreement between the data controllers and the data processor, or between data processors.

Thus, companies that engage vendors for services requiring the processing of personal data are obligated to ensure that such vendors comply with the provisions of the Act. In addition, the companies must have specific data protection agreements with such vendors or ensure that the contract for service with such vendors include data protection clauses.

Sensitive Personal Data

Sensitive personal data is defined in the Act as personal data relating to an individual's genetic and biometric data; race or ethnic origin; religious or similar beliefs such as those reflecting conscience or philosophy; health status; sex life; political opinions or affiliations; trade union memberships; or any other information prescribed by the NDPC Commission, as sensitive personal data.

While the definition of sensitive personal data appears plain and specific, it is not devoid of ambiguity. For instance, it is unclear whether 'similar beliefs such as those reflecting conscience or philosophy' would include notions of personal moral code or values governing a person's personal lifestyle, or whether a record in an employee's personnel file that he or she has expressed a negative view of a colleague's political beliefs classifies as information of that employee's political opinion.

The Act also provides that a data controller or data processor must have proper grounds for processing sensitive personal data and these grounds include: the data subject has consented to the processing for the specific purpose for which it will be processed; processing is necessary for the establishment, exercise, or defense of a legal claim, obtaining legal advice, or conduct of a legal proceeding; or is necessary for reasons of substantial public interest, on the basis of a law, which shall be proportionate to the aim pursued, and provides for suitable and specific measures to safeguard the fundamental rights, freedoms and interests of the data subject; or the processing is carried out for purposes of medical care or community welfare, and undertaken by or under the responsibility of a professional or similar service provider owing a duty of confidentiality.

Personal Data of children or persons lacking legal capacity

Where a data subject is a child or a person lacking the legal capacity to consent, a data controller must obtain the consent of the parent or legal guardian of the child or person. Such consent is however not required where the processing is required to protect the vital interests of the child or person; carried out for educational, medical or social care purpose by a professional or similar service provider owing a duty of confidentiality; or necessary for proceedings before a Court relating to the individual.

Data Protection Officers and Data Protection Compliance Services

The Act requires a data controller of major importance to have a designated Data Protection Officer ('**DPO**') and such DPO maybe an employee of a data controller or engaged by a service contract. The Act also empowers the NDPC to license persons to monitor, audit and report on data controllers and data processors' compliance with the Act and regulations issued by NDPC.

Data Subject's Rights

The Acts establishes several rights of the data subject and these include the data subject's right to right to withdraw consent to the processing of his/her personal data; right to object to the processing of data subject's personal data and right to data portability amongst others.

The Act also gives data subjects the right not to be subject to decisions based solely on automated processing of personal data. However, this would not be applicable where the decision is required for the performance of a contract between the data subject and the data controller; authorised by law or by consent of the data subject. It should be pointed out that this right would only apply where the decision is based solely on automated means. Thus, any form of human intervention, no matter how minute, will be sufficient to overcome this right.

Data Security

The Act imposes obligations on data controller and data processors to develop security measures to protect the personal data of data subject in their possession. Where there is a breach of personal data being stored by a data processor, the data processor must, on becoming aware of the breach, notify the data controller or data processor that engaged it of the breach and respond to all information requests from the data controller or data processor that engaged it, as they may require to comply with the Act.

Furthermore, a data controller must notify the NPDC, within 72 hours of becoming aware of any data breach that is likely to result in a risk to the rights and freedoms of individuals of such breach. In addition, a data controller must immediately notify a data subject of any data breach that is likely to result in a high risk to the rights and freedoms the data subject. It necessary for companies take note of these reporting obligations so as not to contravene the Act in the event of a data breach.

The Act does not clarify what qualifies as 'risk' and 'high risk'. As such pending when the NDPC advises on thresholds of 'risk' and 'high risk', it may, as an abundance of caution, be advisable for companies to report all data breaches as stipulated by the Act.

Transfer of data to a foreign country

The Act provides that a data controller or data processor shall not transfer or permit the transfer of personal data from Nigeria to another country except the recipient of such personal data is subject to a laws that provide an adequate level of protection such as those in the Act. Also, a record of the basis for an offshore transfer of personal data and the adequacy of protection of the personal data must be made by the data controller or data processor.

The underlay of the offshore transfer of data provisions is the assessment of whether the foreign country offers an adequate level of protection of personal data. The Act provides for: (a) the criteria for assessing adequate protection; (b) empowers the NPDC to issue guidelines on the assessment; and, (c) allows the NDPC determine whether a country, region affords an adequate level of protection for personal data.

The Act sets out the conditions for offshore transfer of personal data to a country lacking

adequate protection and these conditions include transfer on the data subject's consent; transfer due to contractual requirements and the transfer is for the data subject's sole vital interest.

Registration of Data Controllers and Data Processors of major importance

Data controllers and data processors of major importance are required to register with NPDC within 6 months of the commencement of the Act or on becoming a data controller or data processor of major importance. A 'data controller of major importance' is one that is domiciled, resident in, or operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria as the NDPC may prescribe; or such other class of data controller or data processor that process personal data of particular value or significance to the economy, society or security of Nigeria as the NDPC may designate.

Companies would have to await the NDPC's guidance on the qualification thresholds for data controllers and data processors of major importance to ascertain whether they qualify as one and once it is determined that an entity qualifies as a data controller and data processor of major importance, then registration with the NDPC is mandatory.

Enforcement and Legal Proceedings

In order to ensure that data controllers and data processors comply with their obligations under the Act, the Act establishes an enforcement framework through the provision of a compliant and investigation procedure.

Accordingly, a data subject may complain to the NDPC about a data controller or data processor's breach of the Act and the NDPC may investigate if it is of the view that the complaint is not frivolous. The NDPC may also on its own volition investigate a data controller or data processor suspected of breaching the Act.

The NDPC can also make compliance orders against a data controller or data processor who has breached the Act as well as make any appropriate enforcement order or impose a sanction on the data controller or data processor. The penalties payable by a data controller or data processor for breaching the Act are: (i) higher maximum amount of ₦10,000,000.00 or 2% of the annual gross revenue of the preceding year or (whichever is greater) in the case of data controllers or data processors of major importance; and (ii)standard maximum of ₦2,000,000.00 or 1% of the annual gross revenue of the preceding year or (whichever is greater) in the case of ordinary data controllers or data processors.

These fines are similar to those prescribed under the NDPR, but the power of the NDPC to impose these fines is debatable due to the recent judicial Court decisions restricting the imposition of fines by administrative bodies.

In addition, data subjects who have suffered injury due to a data controller or data processor's breach of the Act to pursue civil remedies against such data controller or data processor. Thus, aside from the fines payable by a company for breach of the Act, companies are can now be exposed to civil liability for data breaches. In is therefore important for companies to adhere to the provisions of the Act as well as ensure that adequate steps are taken

to protect personal data in their possession to avoid financial exposure.

Any person dissatisfied with an order of the NDPC may apply to the Court for judicial review of such order within 30 days of it being made. It is important to note that the Act provides for a month's pre-action notice before a suit can be instituted against NDPC. A person seeking a judicial review of an NDPC order must therefore bear this in mind to avoid being statutorily barred from seeking such review.

Conclusion

The enactment of the Act is long overdue in Nigeria and aligns Nigeria's data protection and privacy rules with international standards. The Act's enactment further strengthens the right to privacy guaranteed in the Nigerian Constitution as it provides a statutory and legal framework for the protection of personal data and safeguarding privacy rights.

FOR MORE INFORMATION PLEASE CONTACT:

OAB BARRISTERS & SOLICITORS
21, Forsythe Street, Off Hawley Street, Lagos
+ 234 (1) 4538608 | +234-0-9031636416
info@oab-law.com | www.oab-law.com

DISCLAIMER

Please note that this review is for informational purposes only and does not constitute legal advice. If you require specific legal advice tailored to your circumstances or have any questions or concerns arising from the review, kindly contact us at your earliest convenience.