SAFEGUARDING DATA UNDER THE NIGERIA DATA PROTECTION ACT: KEY COMPLIANCE PRINCIPLES FOR DATA CONTROLLERS AND PROCESSORS

abcs Alert

Volume 6 September 2025

Honoré de Balzac, the French novelist and playwright once said "Laws are spider webs through which the big flies pass and the little ones get caught."

This statement may sometimes explain some of the failings of modern-day legal systems where laws can at times be selective and at other times impose unduly burdensome compliance obligations on small businesses struggling for survival while bigger corporations are let off the compliance hook.

The reality however is that the reverse seems to be the case under the data protection regime in Nigeria, contrary to Honoré de Balzac's statement. It can be said that the Nigeria Data Protection Act 2023 is not selective in the enforcement or application of its key provisions in relation to organizations handling data of Nigerians.

On the contrary, it could in fact be argued that the Act ensures that all organizations acting as data controllers and processors, whether major or minor, processing the personal data of Nigerians are "webbed" in its stringent regulatory guidelines and that none takes lightly the duty of safeguarding the fundamental right to privacy of Nigerians as provided under the constitution in their data processing activities.

Data controllers and processors who process the personal data of Nigerians are required to comply with the provisions of the Nigerian Data Protection Act 2023, whether they reside in Nigeria or outside Nigeria.

The Act defines personal data under section 65 which is the Interpretation section of the Act as information relating to an individual who can be identified directly or indirectly by reference to the information collected. The Act goes further to list the categories of information by which an individual can be identified.

The Requirement for Appointment of a Data Protection Officer

The Act, for the purposes of compliance with the requirement of appointing a data protection officer, draws a distinction between data controllers and processors of major importance and those not of major importance.

Data controllers and data processors of major importance are mandated to appoint a data protection officer who will advise them on compliance with the provisions of the Act with regard to their processing activities and act as the organization's contact point for the commission with respect to issues relating to data processing. For data controllers and processors not of major importance, the requirement for appointing a DPO is discretionary.

Although the Act does not specifically define who a data controller or processor of major importance is, reference however is made to data controllers and processors who engage in the processing of personal data of particular value or significance to the economy, society, or security of Nigeria as the Commission may designate, which it has taken steps to do, under the recent 2024 guidance notice where controllers and processors are designated as Ultra High Level, Extra High Level, and Ordinary High Level, with differing levels of compliance obligations imposed on them.

These controllers and processors besides registering with the Commission and filing annual audit returns where applicable, are mandated to comply with the key provisions of the NDPA touching on processing principles.

Under the Act, there are six critical principles to which all organizations processing apersonal data are subject and these principles must be observed in the processing such data, whether data controllers and processors of major importance or not.

These principles are as follows:

#1 Lawfulness, Fairness, Transparency

These tripartite principles form the foundation of all legitimate data processing in Nigeria. Reference to these principles can be found in section 24(1)(a) of

the Act which enjoins data controllers or processors to ensure that personal data is processed in a fair, lawful, and transparent manner.

Lawfulness as a basis for the processing of personal data requires that the processing be traceable to any of the six specific criteria or reasons for the processing of personal data as laid down in the Act.

These six criteria under the Act include;

i. Consent: Obtaining the explicit consent of the data subject prior to the processing

ii. Performance of contract: the processing must be necessary for the performance of a contract with the data subject

iii. Compliance with legal obligation: the processing is required for compliance with a legal obligation to which the data controller or processor is subject.

iv. Protection of vital interest: the processing is essential to protect the vital interest of the data subject or another person.

v. Performance of a public task: the processing is necessary to carry out a task in the public interest or the exercise of an official authority vested in the controller/processor.

vi. Legitimate interests: the processing is done for the purposes of the controller's or processor's legitimate interests or by a third party to whom the data is disclosed

Fairness as a tenet for processing of personal data means that the data controller or processor handles the data in ways that the data subject would reasonably expect and not to use the data in ways that might unjustifiably affect their interests. It also means giving data subjects control and choice over what data is collected, how, if, or when it is processed, and why it should be collected and processed at all.

Transparency requires that data subjects be provided with clear and understandable information regarding the collection, purpose, and processing of their personal data. This is in line with the data subject's right to be informed and should be done at the point of collection of their personal data through the use of a privacy notice.

#2 Purpose Limitation

The principle of purpose limitation requires data controllers and processors to collect data for specified, explicit, and legitimate purposes and to restrict or limit the processing of personal data collected to the original purposes for which the data was collected. Where it is to be further processed or put to new purposes, additional consent of the data subject must be sought unless the new purpose is compatible with the original purpose.

#3 Data Minimization

This principle is to the effect that personal data collected by a controller or processor should be adequate, and relevant and must be limited to the minimum necessary for the purposes for which the personal data was collected. A data controller and processor is therefore prohibited from collecting more data than necessary for any stated purpose.

#4 Accuracy

The principle of accuracy mandates data controllers and processors to ensure that the personal data collected is accurate, complete, and not misleading. Controllers and processors are further required to update such data where necessary and to provide the data subjects the means of updating their data where possible. This is in line with the right of rectification of personal data by data subjects.

#5 Storage Limitation

This requirement means that data controllers and processors are to store the data collected for no longer than is absolutely needed for the purpose for which it was collected. This may also require data controllers and processors to provide data subjects the means of deleting their personal data collected where it is no longer relevant or useful. This is otherwise known as the right to be forgotten.

#6 Integrity, Confidentiality and Availability

The tripartite principles of integrity, confidentiality, and availability, otherwise known as the "CIA triad" in cybersecurity, are technical standards or measures to be implemented by data controllers and processors to protect the integrity, and confidentiality of personal data collected from tampering, unauthorized access or accidental disclosures or loss as well as guarantee the access of data subjects to their stored data with the data controllers or processors.

Organizations that process personal data can observe the principles of integrity, confidentiality, and availability as stated by the Act by implementing organizational and technical measures to secure the personal data collected.

It should be said that implementing these organizational and technical measures may require the involvement or participation of IT and cybersecurity professionals.

The following are some measures a data controller or processor can implement to protect personal data collected and stored by them.

i. Implementing security controls such as role-based access

ii. Utilizing data loss prevention tools and creating a backup of stored data

iii. Implementing complex passwords to deny access to confidential data by unauthorized individuals

iv. Protecting confidentiality through anonymization, pseudonymization, and aggregation of collected data with personal identifiers

v. Implementing availability controls such as fault tolerance, clustering, and backups to minimize disruptions and ensure availability of personal data.

In conclusion, implementing organizational measures may also dictate that data controllers and processors implement policies, procedures, and practices for identifying potential risks to data security and mitigating them.

It may also require the data controllers and processors to implement incident management practices and procedures for early detection of data

breaches and to report such breaches to the affected individuals and the Nigeria Data Protection Commission within 72 hours of their knowledge of such breaches.

For data organizations engaged in data processing, it is important to ensure they adhere to these principles in all aspects of their operations as non-compliance can attract serious fines under the NDPA, ranging from enforcement action, fines of up to N10,000,00 or 2% of annual gross revenue in the preceding year as well as civil and criminal actions in Court.

"With decades of experience and expansive global network, we are predominantly focussed on providing top notch business services to our multinational and international clients

5 /7 Ademola Street,
off Awolowo Road
South West Ikoyi, Lagos, Nigeria

19 Kolda Street,
Off Adetokunbo Ademola Crescent
Wuse II, Abuja, Nigeria

(+234) 906 902 2222
(+234) 906 903 3333
(+1) 917 809 4981
(+44) 203 807 9070

abcs-global.com
solutions@abcs-global.com