




WHAT YOU NEED TO KNOW ABOUT THE NIGERIAN DATA PROTECTION ACT, 2023



Available now
to read **FREE**
online

www.dealhqpartners.com

 dealhqpartners

INTRODUCTION

As technology and digital innovation continues to advance, the volume of data generated and exchanged by users of the internet, mobile/web applications and other digital devices has raised the security of personal data to the status of “matter of national concern” in Nigeria.

On the 14th of June 2023, the President of the Federal Republic of Nigeria, signed into Law, the Nigerian Data Protection Act (the Act) thereby establishing by statute, the Nigerian Data Protection Commission; which is entrusted with the power to make and enforce regulations for the protection and security of the personal data of Data Subjects in Nigeria.

1. SCOPE OF THE LAW

The Act provides the legal framework for the establishment of the Nigeria Data Protection Commission, the regulation of the processing of personal data of Data Subjects, and for other related matters. The objective of the Act is to safeguard the constitutional right of Data Subjects in Nigeria as relates to the processing activities undertaken by Data Processors or Data Controllers. A *Data Controller is a person, organization, or a statutory body who determines the purposes for, and the way Personal Data is processed or is to be processed. Consequently, a Data Processor is one who processes the data in the manner prescribed by a Data Controller*).

2. WHO DOES THE ACT APPLY TO?

The Act applies to and is binding on Data Controllers or Data Processors who are either:

- a. Resident or operating in Nigeria;
- b. Processing data within Nigeria; or
- c. Processing data of Data Subjects in Nigeria.

3. EXEMPTION

Data Controllers or Processors who fall into any of the underlisted categories are exempted from the application of the Act:

- a. One or more individuals who process personal data solely for personal or household purposes;
- b. Data Controllers or Processors who deal with/process personal data which have been prescribed for exemption by the Commission.

4. ESTABLISHMENT OF THE NIGERIA DATA PROTECTION COMMISSION

The Act establishes the Nigeria Data Protection Commission as an independent body responsible for prescribing regulations, codes, guidelines, and procedures in furtherance of its functions geared towards the enhancement of personal data protection.

The overall policy direction of the affairs of the Commission shall be controlled by a governing council which shall consist of seven people headed by a Chairman who shall be a retired judge of a superior court of record. All seven members of the governing council shall be appointed by the President on the recommendation of the Minister.²

5. **LAWFUL BASIS FOR PROCESSING PERSONAL DATA**

Personal Data of a Data Subject can only be processed when a lawful basis for such has been established. The Act like other Data Privacy statutes (such as the GDPR) recognizes that Lawful Basis shall be deemed established in the following scenarios:

- a. Consent: Data Subject's consent has been procured and the consent has not been withdrawn;
- b. Contract: Processing the personal data is necessary or the performance of a contract for which the Data Subject is a Party;
- c. Legal Obligation: Processing the data is necessary for compliance with a legal obligation to which the Data Controller or Processor is subject;
- d. Public Interest: Processing the personal data is necessary for public interest purposes or in exercise of official authority vested in a controller;
- e. Vital Interest: to protect a life;
- f. Legitimate Interest: Where the processing of personal data of a data subject is necessary in the legitimate interest of the processor or another third party.

Relatedly, even after Lawful Basis is established, every Data Processor is expected to adhere to these general principles:

- a. Personal Data must be processed in a fair and transparent manner;
- b. Personal Data must be collected for a specified and legitimate purpose; and must not be further processed in a manner or for a purpose incompatible with that which has been specified;

- c. Personal Data collected must be limited to that which is adequate and relevant for the purpose for which it is collected;
- d. Personal Data must be retained only for only as long as is necessary to achieve the Lawful Basis for which it was collected;
- e. Personal Data must be processed in a manner that guarantees the security of personal data against loss, unlawful processing, destruction loss or damage.
- f. Personal Data is processed for the purpose of a legitimate interest by a data controller or third party to which the data is disclosed.

6. **KEY PROVISIONS TO NOTE**

Amongst other things, the following mandatory provisions are to be noted by and complied with by all Data Controllers and Processors:

- a. **MANDATORY APPOINTMENT OF A DPO**
All Data Controllers and Processors of major importance³ are now mandated to appoint a designated Data Protection Officers (DPO) with expert knowledge of data protection laws and practices and who may either be an employee of the organization or engaged under a valid service contract⁴.
- b. **DATA PROTECTION IMPACT ASSESSMENT**

Every Data Processor or Controller who envisages that any of its processing activity is likely to violate or result in high risk to the rights and freedom of Data Subjects by virtue of its nature, scope, context and purpose; is mandated to conduct a data protection impact assessment. It is expected that the Commission will issue guidelines to establish the categories of processing

² Part II and III of the Act.

³ A Data Controller or Processor domiciled, resident in or operating in Nigeria who processes or intends to process personal data of such

number of Data Subject within Nigeria as the Commission may prescribe as being of major importance.

⁴ Section 33 of the Act.

which will now require the conduct of data protection impact assessment.⁵

c. REPORTING DATA BREACHES

Every Data Controller is required to notify the Commission within 72 hours of becoming aware of any personal data breach which is likely to result in a risk to the right and freedom of a Data Subject.⁶

d. CROSS BORDER DATA TRANSFER

Cross-Border Transfer of personal data to third parties no longer requires the supervision/consent of the Attorney General of the Federation. Notwithstanding Personal Data of Data Subjects cannot be transferred to a cross border recipient; unless the transferor has satisfied itself that the foreign third-party recipient:

- i. Has a lawful basis for processing such data;
- ii. Has in place a mechanism to ensure adequate level of protection of such data to the extent and level prescribed by the Act.⁷

e. REGISTRATION OF DATA PROCESSORS AND CONTROLLERS

The Act mandates the registration of Data Controllers and Data Processors of major importance with the Commission within six months from the commencement of the Act or of becoming a Data Controller or Data Processor of major importance. The Act also prescribes the process of registration and grants the Commission the power to prescribe the registration fee and to grant exemptions from registration at their reasonable discretion. Furthermore, Registered Processors and Controllers must notify the Commission of any change in the registration details provided.

The Commission is expected to keep a register of Data Controllers and Processors on its website and to update same regularly. When a Data Controller or Data Processor ceases to be one of

major importance, it must notify the Commission who shall remove its name from the register⁸.

f. GENERAL RIGHTS OF DATA SUBJECTS

The Act guarantees Data Subjects the inherent right to:

- a. Obtain from a Data Controller; confirmation as to whether its personal data is being stored or processed and where so; further information on the purpose, nature/category of data being processed, recipients of such data including international/cross border recipients, period for which data will be kept;
- b. Right to demand rectification, erasure or restriction in processing (pending resolution, objection or enforcement of a legal claim) without delay;
- c. Right to decline to give or to withdraw consent;
- d. Right to demand discontinuation of processing (except on grounds of public interest);
- e. Right to lodge a complaint with the Commission;
- f. Right not to be subject to a decision based solely on automated processing of personal data.

g. RIGHT OF AGGRIEVED DATA SUBJECTS TO FILE COMPLAINTS WITH THE COMMISSION

The Act has provided a procedure for Data Subjects whose rights have been violated or is likely to be violated by any Data Controller or Processor; to file a complaint with the Commission⁹. The Commission is mandated to investigate and where it is established that the right of a Data Subject is likely to be violated, the Commission will issue an appropriate compliance order against such Data Controller including:- (1) a warning (2) a directive to comply or (3) a cease and desist order.

⁵ Section 29 of the Act.

⁶ Section 41 of the Act.

⁷ Part IX of the Act.

⁸ Part X of the Act.

⁹ Sections 47, 48 and 49 of the Act.

Where however an actual violation is established; the Commission may issue an enforcement order issuing sanctions against such Data Processor or Controller. Such order may include (1) a directive to remedy (2) a directive to pay compensation (3) order to account for profits made from a violation (4) order to pay penalty which in the case of a Data Controller of major importance will be the higher of NGN10Million or 2% of gross revenue for the preceding financial year. Where the offender is not a Data Controller of major importance, the penalty will be the higher of NGN2Million OR 2% of gross revenue for the preceding financial year. Where Data processor or controller is dissatisfied with the order imposed by the commission, it is at liberty to apply to court for judicial review, within thirty days of the issuance such order¹⁰.

Where an order is defiled, the defaulting Processor or Controller commits an offence and becomes criminally liable upon conviction by a competent court¹¹. The court may also order the Processor or Controller upon conviction to forfeit any economic benefit or financial proceeds in accordance with the Proceeds of Crime (Recovery and Management) Act or any other similar law.¹²

h. JOINT AND VICARIOUS LIABILITY

Directors, Managers, Partners, Secretaries or other similar officer of any convicted Data Processor or Controller shall be deemed jointly and vicariously liable with the organization for any breach or violation or offense under the Act; unless such officer can prove that the offence was committed without his/her knowledge, consent or connivance; and that he/she exercised all such diligence to prevent the commission of the offence. Data Controllers and Data Processors also remain vicariously liable for the acts or omissions of their agents, clerks, servants or employees.¹³

7. LIMITATIONS IN RESPECT OF LEGAL PROCEEDINGS AGAINST THE COMMISSION

Whilst the Commission remains a legal entity which can sue or be sued, Actions against the Commission are required to be instituted within three months of the time in which such cause of action arose and subject to the service of a one month written notice of intention to sue having been served on the Commission. The Act further directs that no execution or attachment process can be issued against the property of the Commission in respect of an action or suit filed against it¹⁴.

8. TRANSITIONAL PROVISION

The Act recognizes and has given legitimacy to all actions (orders, rules, decisions, directions, licenses and authorizations) of NITDA, OR the Bureau done prior to the coming into force of the Act as if they are acts of the Commission itself and they shall remain binding until they are waived, cancelled or repealed by the Commission. This includes specifically, the Nigerian Data Protection Regulation (NDPR) 2019.¹⁵ The Nigeria Data Protection Commission effectively succeeds the erstwhile Nigeria Data Protection Bureau (NDPB) and puts to an end the argument that the NDPB is not statutorily created.

IMPLICATION FOR BUSINESSES IN NIGERIA

It is clear given the priority and attention given to the assent of the by the newly elected President of Nigeria and the Federal Executive Council; that data privacy is recognized as a critical focus area for the Federal Government. It can therefore be fairly deduced that enforcement of the Act will be top of mind for the Government and the Commission.

The Act has further mandated registration for all data processors and controllers within the next six months. Consequently, Businesses operating in Nigeria except where exempt will be required to immediately reposition their protocol of operation to ensure consistent compliance with the Act. Finally, Data Processors and Controllers must keep as top of mind the potential risk of sanctions and criminal liability where they have directly or vicariously violated the rights Data Subjects as guaranteed under the Act.

¹⁰ Section 51 of the Act.

¹¹ Section 50 of the Act.

¹² Section 53 of the Act

¹³ Section 54 of the Act

¹⁴ Part XII of the Act.

¹⁵ Section 64 the Act.

*This Article is written by DealHQ's Technovation and Data Governance Practice Team, DealHQ is a licensed Data Protection Compliance Organization (DPCO). We understand the importance of safeguarding sensitive data and complying with local and foreign data protection laws applicable to your business to protect your organization's reputation and mitigate potential cybersecurity or data violation risks which can have significant financial, legal and systemic implications for your Business. Our service niche includes (1) Data Protection/Governance Advisory (2) Data Protection Compliance Support (3) Data Protection Audit Services and (4) Outsourcing of Data Protection Officers.

About DealHQ

We are an Africa Focused deal advisory/boutique commercial law firm focused on supporting businesses and positioning them to operate efficiently within their market sphere. We are known for our quality service delivery which is focused on attention to detail, creativity, timely execution and client satisfaction.

Our service offering includes: corporate commercial, real estate & construction, finance, capital markets & derivatives, mergers and acquisitions, private equity, infrastructure, technovation and data privacy, agriculture & commodities, business formations & start up support amongst others.

The content of this Article is not intended to replace professional legal advice. It merely provides general information to the public on the subject matter.

Do you need to know more about our Data Privacy Services? You may contact our team on:

✉ Email: info@dealhqpartners.com; clientservices@dealhqpartners.com

☎ Telephone: +234 1 4536427 or +234 9087107575