TEMPLARS

26 June 2023


**Key Contacts**

**Ijeoma Uju**
Partner,
Corporate & Commercial
ijeoma.uju@templars-law.com

**Okabonye Chukwuani**
Associate,
Finance
okabonye.chukwuani@templars-law.com


# Client Alert

## Navigating the New Data Protection Regime: Key Takeaways from the Nigerian Data Protection Act, 2023

### Introduction

As predicted in the Templars Tech Outlook for 2023, the Data Protection Bill 2022 was passed into law last week by President Bola Ahmed Tinubu, making it the first Act focused on data protection in Nigeria. The Data Protection Act, 2023 (the "**DPA**") comes after several attempts by different administrations to legislate on data protection in Nigeria. Up until the signing of the DPA, data protection in Nigeria was largely governed by administrative regulation (specifically, the Nigerian Data Protection Regulation 2019) as there was no substantive law on data protection passed by the National Assembly. The DPA has changed that completely.

**"Our projections for 2023 are that the year will be a landmark year for data protection in Nigeria…We anticipate passage of the Data Protection Bill given the high enthusiasm of the relevant stakeholders about the Bill".**

In light of the new data protection framework in Nigeria, it is critical for businesses (both in the tech sector and in all other sectors) and other stakeholders to familiarize themselves with the changes introduced by the DPA to ensure that they are compliant with the law in data processing activities, as well as ensure adequate protection of the personal data of their customers and employees. The DPA is also relevant to all Nigerian citizens and individuals in Nigeria as it is now the premier law protecting their personal data.

In this client alert, we will examine the DPA side-by-side with the previous National Data Protection Regulation (the "**NDPR**") framework (comprising of the NDPR 2019 and the NDPR Implementation Framework 2020), highlighting the key changes introduced by the DPA and how it affects data protection compliance within and outside Nigeria.

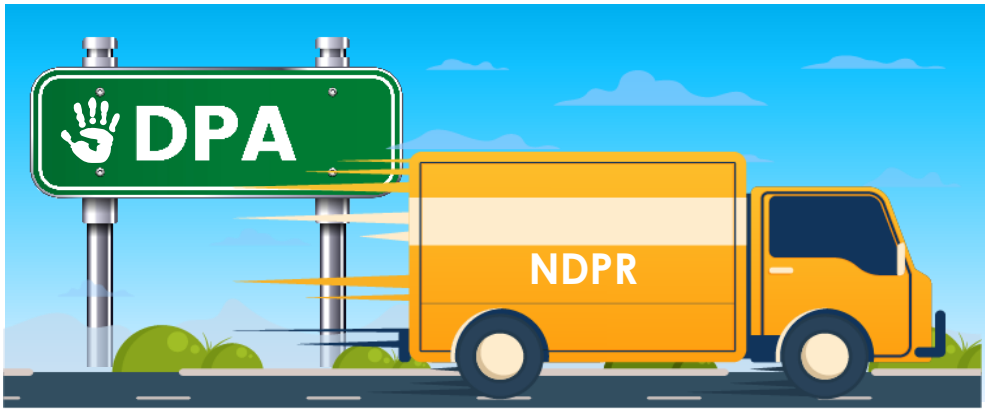
## Key Highlights and Implications

### (a) Status of the NDPR – DPA Takes Priority

The enactment of the DPA in Nigeria has raised some questions about the status of the NDPR. Contrary to what some may have expected or predicted, the NDPR does not automatically fall away with the enactment of the DPA. The DPA preserves all regulations made by the National Information Technology Development Agency ("**NITDA**) or the Nigeria Data Protection Bureau (NDPB) on the subject of data protection prior to the enactment of the DPA. This means that the NDPR and all regulations made under it, remain in force until they are repealed, replaced, amended, or altered.[1]

To balance out the potential areas of conflict or contradictions between the existing framework and the DPA, the DPA also provides that in cases where any law contradicts or is inconsistent with its provisions, the DPA takes precedence.[2] As a result, the DPA effectively supersedes the NDPR as the primary data protection law in Nigeria. Consequently, other guidelines and frameworks developed in accordance with the NDPR, such as the NDPR Implementation Framework 2020 and the Public Institution Guidelines 2020, are subject to the provisions of the DPA.

**However, this does not mean that the NDPR is completely obsolete. Provisions of the NDPR that do not contradict the DPA remain applicable and enforceable.** For example, although the DPA does not contain provisions on annual data protection audit filings, the obligation still subsists by virtue of the NDPR.[3] **Therefore, data controllers who have not yet filed are still required to do so before the extended deadline of 30 June 2023.** It is also important to note that the DPA also grants the new regulator the power to make regulations for the frequency and content of compliance returns.[4] Therefore, the




regulator may choose to retain the current yearly audit filing requirement. However, it is also possible that the regulator will choose to adopt a different approach to compliance reporting.

Another key point to consider is the 'Whitelist', which is not replicated in the DPA. The Whitelist is a list of over 40 jurisdictions (including the EU, UK, USA and others), that Nigeria considers as having adequate data protection laws. Flowing from the reasoning set out

[1] Section 64 (2) (f) of the DPA.
[2] Section 63 of the DPA.
[3] Article 4.1 (6) (7) of the NDPR.
[4] Section 61 (2) (g) of the DPA.

above, the Whitelist will continue to remain valid until the new regulator makes any changes in this respect.

**(b) Change of Data Protection Regulator – Nigeria Data Protection Commission**


Another important change brought about by the DPA is the establishment of the Nigeria Data Protection Commission ("**NDPC**"). The NDPC replaces the Nigeria Data Protection Bureau ("**NDPB**", which itself had replaced the NITDA in February 2022) as the primary regulator for data protection in Nigeria (the NITDA still remains the overall IT regulator in Nigeria). A review of the transition provisions of the DPA shows that what essentially occurs is a mere name change rather than an institutional overhaul as the NDPC inherits the employees, agreements, records, equipment, properties, legal claims and actions, as well as regulations and certifications of the NDPB and NITDA with respect to data protection.[5] However, for the purpose of nomenclature, record keeping, regulatory communications and documentation, data controllers and processors should note that the new regulator for data protection in Nigeria is the NDPC and all compliance and any filing obligations should be carried out with this in mind.

**(c) Data Controllers/Processors of Major Importance – Registration Required**

The DPA introduces a new concept called data controllers/processors known as Data Controllers/Processors of Major Importance ("**DCMI/DPMI**"). Under the DPA, DCMIs/DPMIs are subject to further obligations in addition to those imposed generally on data controllers/processors. These include the requirement to appoint an expert data protection officer[6] and a new requirement (which did not exist under the NDPR) **to register with the NDPC**.[7] Additionally, in cases of a breach of the DPA, DCMIs/DPMIs are subject to higher fines than other data controllers/processors.[8]

What would qualify an entity to be a DCMI or DPMI? The DPA appears intentionally vague and leaves it up to the NDPC to set the parameters for determining entities which qualify as DCMIs.[9] Until a regulation is issued in this respect, the uncertainty may create a compliance challenge for businesses and organizations, as they do not know which obligations they are required to meet.

[5] Section 64 (2) of the DPA.
[6] Section 32 of the DPA.
[7] Section 44 of the DPA.
[8] Section 49 of the DPA.
[9] The DPA defines "data controller or data processor of major importance" as a data controller or data processor 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 Commission may prescribe, or such other class of data controller or data processor that is processing personal data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate.

### (d) The Recognition of Legitimate Interest (LI) – A New Lawful Basis for Processing Data


One of the notable shortcomings of the NDPR was its failure to recognize the legitimate interests of the data controller ("**LI**") as a lawful basis for processing personal data. The DPA has now rectified this by recognizing LI as a lawful basis. However, it is important to note that the LI test under the DPA varies slightly from the LI test under the General Data Protection Regulation ("**GDPR**").

Under the DPA, for a data controller to rely on LI as its lawful basis, it must show that:

(i) The interest does not override the fundamental rights, freedoms, and interests of data subjects;
(ii) The interest is not incompatible with other lawful bases of processing under the DPA; or
(iii) The data subject has a reasonable expectation that personal data would be processed in the manner envisaged.[10]

The GDPR also adopts a three-pronged approach: identifying a legitimate interest, conducting a necessity assessment, and conducting a balancing test. The controller must demonstrate a valid purpose for data processing, ensure it is necessary for achieving that purpose, and assess whether the individual's fundamental rights and freedoms outweigh the controller's interests.

Businesses coming from other jurisdictions (or businesses operating in other jurisdictions but processing Nigerian personal data), particularly the EU, need to take note that the metrics for relying on LI in Nigeria differ from what is obtainable under the GDPR and should thus be aware of this difference, especially if they intend to rely on this ground of processing in Nigeria.

### (e) Sensitive Personal Data – Expansive Rules for Processing

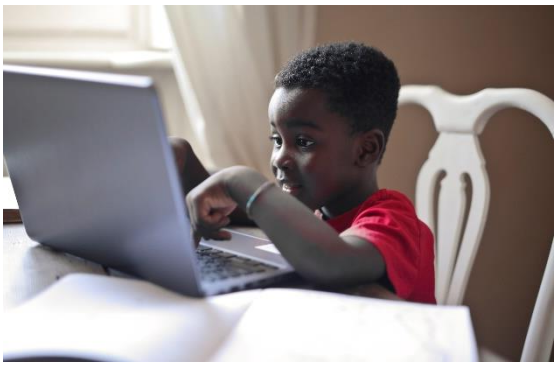
The DPA expressly defines sensitive personal data, which includes genetic and biometric data, race or ethnic origin, religious beliefs, health status, etc. The DPA also provides for extensive and specific grounds for when such sensitive data can be processed. These include, but are not limited to, where consent has been obtained (and not withdrawn); for compliance with social security or employment laws; to protect vital interests; for medical care; for reasons of public health; etc.[11] It is important for data controllers and processors to note the categories of data deemed "sensitive" and have a reliable ground of processing when handling such data.

An interesting change from the definition of sensitive personal data under the NDPR, is that "sexual orientation" has been replaced with "sex life" within the meaning of "sensitive personal data" in the DPA[12]. It is not exactly clear what this means, and whether it is safe to assume that personal data around an individual's sex life would mean the same as their sexual orientation. It is possible that this was done to expand the scope of coverage of sensitivity here to include not only sexual orientation, but also intimate data

[10] Section 25 (2) of the DPA.
[11] Section 30(1) of the DPA.
[12] See the definition of "sensitive personal data" under Section 65 of the DPA.

(such as pictures, videos, etc.) around a person's sex life within the protection of "sensitive personal data".

**(f) Children's Personal Data – New Safeguards**



The NDPR framework did not have substantial provisions for protecting the personal data of children. It is positive to see that the DPA has taken a big step towards addressing this gap.

Processing data based on consent of a child (a person less than 18) requires consent of their parent or legal guardian[13]. Data controllers are also now required to implement age-gating and consent verification mechanisms, based on any government valid identification (i.e. driver's licence, national identity number, international passport, etc.)[14] We also expect further guidelines from the Commission to address situations where a child aged 13 or older is specifically requesting the provision of electronic services.[15]

In our view, the DPA provisions (along with the future guidelines) should address the modalities around children's use of the internet and applications, the processing of such data, and the appropriate rules and safeguards, while not totally inhibiting the ability of children / young teens to access digital resources and services.

**(g) Cross Border Data Transfer under the DPA – Similar to the NDPR**

The DPA introduces a similar (but more comprehensive) approach to cross-border data transfers compared to the NDPR, which relied largely on inferences from the Implementation Framework.

Under the DPA, there are two main bases for cross-border data transfers: (a) the "Adequacy protection" rule[16], which includes the recipient's law, binding corporate rules, contractual clauses, code of conduct, or a certification mechanism, or in the absence of such adequacy protection; (b) one of the conditions outlined in section 43

[13] Section 31(1) of the DPA.
[14] Sections 31(2) and (3) of the DPA.
[15] Section 31(5) of the DPA.
[16] Put simply – where it is determined that the recipient's jurisdiction / sector has adequate rules protecting personal data.

of the DPA must be met.[17] This differs slightly from the GDPR, which has three broad bases for cross-border transfers: adequacy decisions, appropriate safeguards, and specific derogations with distinct parameters.

The NDPR Whitelist appears to remain valid for now as an adequacy reference for the DPA.

**(h) Regulations and Guidelines – NDPC Clarity Required for Implementation**

One notable aspect of the DPA is its use of broad language and open-ended provisions, allowing the NDPC ample flexibility to issue guidelines, regulations, and directives that provide specific details and instructions for implementing these provisions.

Consequently, for many provisions in the DPA to take effect e.g. provisions relating to DCMIs/DPMIs, data protection impact assessments, compliance filings, cross-border data transfers, personal data breaches etc., it is essential for the NDPC to issue timely guidelines that outline the implementation process.

There are concerns about the timely implementation of the DPA's provisions and particularly about how much time it would take for such guidelines to be issued especially considering the track record of Nigerian data protection regulators in issuing guidelines and directives. Nevertheless, there is optimism that with a dedicated regulatory body fully backed by an act of the national assembly, the implementation of the Nigerian data protection framework will become more seamless, effective, and efficient.

**(i) Penalties – Administrative / Criminal Redress and Vicarious Liability**

A common question for stakeholders is whether a regulator would immediately look to impose administrative fines or criminal enforcement, or whether a grace period would apply. The DPA answers this clearly – the Commission does have powers to issue enforcement orders in the form of warnings, compliance demands or cease and desists[18], but the alleged defaulter is to be given a grace period to implement the measures required. Administrative fines for breach of the DPA can be imposed following investigation.

The applicable penalties differ depending on whether the offending controller or processor is of "major importance" or not. For those that are of major importance, the fine shall be the higher amount between N10,000,000 or 2% of the controller/processor's annual gross revenue in the preceding financial year. For those that are not of major importance, the fine is the higher amount between N2,000,000 or 2% of the controller/processor's annual gross revenue in the preceding financial year.[19]

[17] Section 41 (1) of the DPA.

Under section 43 of the DPA, a data controller or data processor shall only transfer personal data from Nigeria to another country under certain circumstances, including but not limited to where consent has been properly obtained; the transfer is necessary for the performance of a contract, etc.

[18] Section 47 of the DPA.

[19] Section 48 of the DPA.

Criminal sanctions can also be imposed for continued failure to comply with an enforcement order. The criminal fines are the same amounts described above (applicable upon conviction) with the possibility of imprisonment for convicted officers of the controller / processor. Lastly, controllers or processors can be held vicariously liable for acts or omissions by agents or employees.[20]

## Conclusion

The enactment of the DPA marks a significant milestone in Nigeria's efforts to regulate data protection. It introduces crucial changes that demand careful attention from stakeholders, both within and outside Nigeria, to ensure they meet their obligations and remain compliant with the law. By familiarizing themselves with the key changes and seeking expert guidance, businesses can navigate the evolving Nigerian data protection framework, protect the privacy of their customers and employees, and establish trust in an increasingly data-centric business environment.

That said, there are still key regulatory clarifications needed on important issues and terms under the law. Additionally, certain provisions of the DPA raise questions, such as the potentially unlimited right to withdraw consent, ambiguities around the right to object to processing, and the vagueness around the designation of data controllers / processors of "major importance", to name a few. We look forward to the Commission's prospective guidelines and clarity on these and other matters of importance.

### Authors

**Ijeoma Uju**
Partner,
Corporate & Commercial
ijeoma.uju@templars-law.com

**Okabonye Chukwuani**
Associate,
Finance
okabonye.chukwuani@templars-law.com

**Victoria Oloni**
Associate,
Corporate & Commercial
victoria.oloni@templars-law.com

**Tomisin Olanrewaju**
Associate,
Finance
tomisin.olanrewaju@templars-law.com

[20] Section 53 of the DPA.