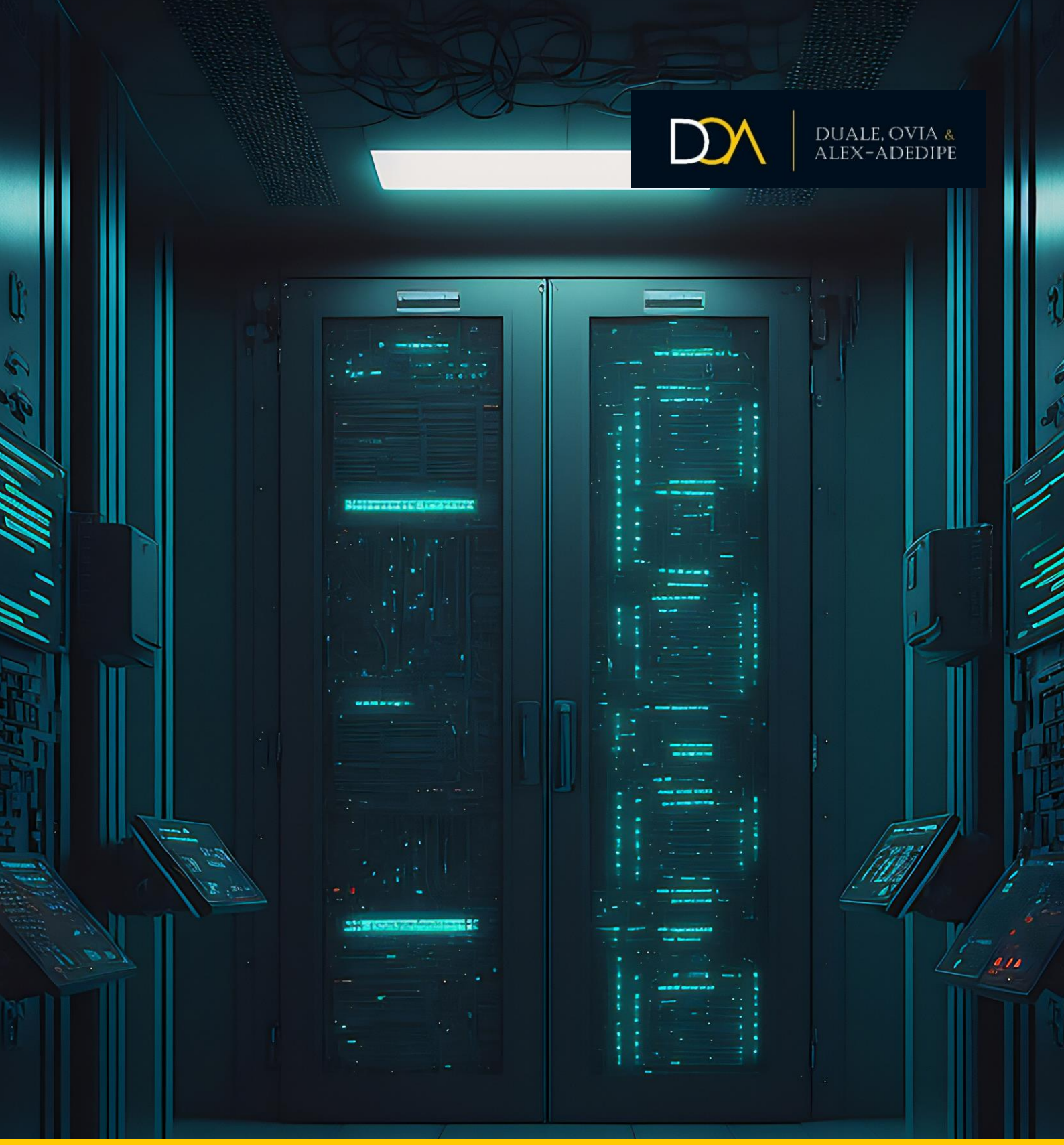

Highlights of Business Compliance under the Nigeria Data Protection Act, 2023

www.doa-law.com

1. Introduction

In a bid to align Nigeria with the global regulatory trend on personal data and to enjoy a competitive edge at the global stage, the Nigerian Data Protection Act, 2023 (The "Act") was given presidential assent on 14th June 2023.

The Act introduced innovative provisions which are geared toward safeguarding and guaranteeing the right and freedom of data subjects under the Nigerian Constitution. The intendment of the Act appears to bring to rest the controversy on whether data subjects' rights are fundamental human rights, as the question is answered in the affirmative. The Act also established the Nigerian Data Protection Commission (the "**Commission**") and provides complete and comprehensive principles of data protection for the first time in Nigeria.

Major players under the Act are entities, businesses and individuals who act either as data processors or data controllers. This article highlights compliance obligations for these companies along with innovative provisions of the Act.

COMPLIANCE OBLIGATIONS FOR BUSINESSES

2. Complying with the Rights of Data Subjects

Companies are encouraged to understand and comply with the rights of data subjects. The Act provides various rights to data subjects and further recognized these rights as fundamental human rights[1]. These rights include the right to inform data subjects on the entirety of the processing activities[2]; right to request access to personal data[3]; right to correct inaccurate personal data[4]; right to delete, erase or suppress personal data [5]; right to restrict data processing[6]; right to withdraw consent[7]; right to object to the processing of personal data[8]; right not to be subject to automated decision making[9]; right to receive personal data or have it transmitted to another data controller in a structured, commonly used and machine-readable format[10].

[1] Section 1(a) Nigeria Data Protection Act, 2023.
[2] Section 27, Nigeria Data Protection Act, 2023
[3] Section 34, Nigeria Data Protection Act, 2023
[4] Section 34(1)(c) Nigeria Data Protection Act, 2023
[5] Section 34(1) (d) & (2) Nigeria Data Protection Act, 2023.
[6] Section 34(1)(e) Nigeria Data Protection Act, 2023.
[7]Section 35(1) Nigeria Data Protection Act, 2023.
[8] Section 36(1) Nigeria Data Protection Act, 2023
[9] Section 37 Nigeria Data Protection Act, 2023
[10] Section 38 Nigeria Data Protection Act, 2023

DUALE, OVIA & ALEX-ADEDIPE

In a bid to align Nigeria with the global regulatory trend on personal data and to enjoy a competitive edge at the global stage, the Nigerian Data Protection Act, 2023 was given presidential assent on 14th June 2023.

3. Data Movement

i. Portability of data

To comply with data subject's right to portability, companies are enjoined to install or implement measures that will enable data subjects to receive personal data from the company or request for the data to be transmitted directly from the company to another company, without delay.

ii. Personal data transfer

Companies that intend to move data out of Nigeria (for instance, by using a cloud facility domiciled in another country) may freely do so to countries recognized in the Whitelist contained the Implementation Framework. Countries in the Whitelist are regarded as having adequate data protection laws. These companies should also adopt appropriate standard contractual clauses or other mechanisms such as code of conduct or certification mechanisms where applicable[11]. Where adequacy protection becomes impossible or absent, a company may rely on other lawful bases such as obtaining the consent of the data subject to transfer personal data, ensuring that the transfer is necessary for the performance of a contract between the company and the data subject; ensuring that the transfer is for the sole benefit of the data subject, ensuring that the processing is tied to an important public interest or for the defense of legal claims among others[12].

4. Privacy Notice/Policy

Businesses that deal with personal data must publish privacy notices at every point where personal data is collected. The privacy policy will detail how personal data is processed by the company, including technical and organizational measures adopted by the company to ensure adequate protection of personal data. The privacy notice must contain the minimum requirements as prescribed by law.

5. R.A.C.I.

The Act requires personal data to be processed in a manner that guarantees its confidentiality and integrity. To meet this requirement, it is recommended that companies adopt the RACI mechanism in relation to processing data. RACI is an acronym for Responsible, Accountable, Consulted, and Informed. It is a matrix that clarifies individuals or groups who are responsible for the successful completion of a project. It ensures that the company has the organizational/hierarchical structure and technical controls to protect personal data in its possession from foreseeable hazards and breaches such as cyberattacks, manipulations, theft, and other exposures.

[11] Section 41Nigeria Data Protection Act, 2023
[12] Section 43 Nigeria Data Protection Act, 2023

6. Data Protection Impact Assessment (DPIA)

A DPIA is a process designed to identify the risks and impact of the envisaged processing of personal data[13]. It is important for companies to have a DPIA policy to guide them in assessing if data processing activities require a DPIA at any point in time. Where processing data will likely lead to high risk to the rights and freedoms of data subjects by virtue of its nature, scope, context, and purposes, a company is expected to carry out a DPIA prior to processing of personal data (DPIA)[14]. A Company is expected to undertake DPIA if it engages in one or more of the following projects:

a). Evaluation or scoring (Profiling);
b). Automated decision-making with legal or similar significant effect;
c). Systematic monitoring;
d). Sensitive data or data of a highly personal nature;
e). When Data processing relates to vulnerable or differently abled Data Subjects; and
f). When considering the deployment of innovative processes or the application of new technological or organizational solutions.

7. Data Subject Access Request (DSAR)

Data subject access request (DSAR) is an offshoot of the right to access. The law empowers a data subject to obtain from a company without delay confirmation as to how his/her personal data is being processed and to obtain a copy of such personal data without delay[15]. Therefore, companies are obligated to put technical and organizational measures in place to ensure they respond to data subject access requests. To comply with this requirement, companies ought to maintain a DSAR policy that will guide them in implementing a DSAR promptly.

8. Data Protection Audit

The Nigeria Data Protection Regulation (the "**NDPR**") requires every company with a processing capacity of over 2000 data subjects to conduct data protection audits and file audit reports on or before 15th March of each year. Among other things, the audit will enable the company to identify compliance gaps in its processing activities. While the Act is silent on the threshold for data audit, it preserved the provisions of the NDPR which makes the 2000 threshold in NDPR valid and subsisting until repealed[16].

[13] Section 28(4) Nigeria Data Protection Act, 2023
[14] Section 28 Nigeria Data Protection Act, 2023
[15] Section 34(1) Nigeria Data Protection Act, 2023.
[16] Section 64(1)(f) Nigeria Data Protection Act, 2023

9. Registration with the Commission

Section 44 of the Act requires a controller and processor of major importance to register with the Commission within 6 months of the commencement of the Act (i.e., December 2023). The Act defined major importance, however the definition failed to provide factors that designate a company as having major importance.

10. End User Interactive Platform

Section 24(e) and 34 (1)(d) of the Act require companies to ensure the accuracy of personal data in their custody. Therefore, companies are enjoined to create an end user interactive platform or mechanism that will enable their customers to correct or update their personal data, especially where there are changes in status quo. Also, platform-based companies need to develop adequate mechanisms on their platforms that will enable them to obtain a valid consent from data subject on their websites and online platforms like the “tick box” or “I agree” button, and sign form, among others. Companies may also consider procuring consent management vendors to enable them to obtain valid consent. Where the consent is to be obtained manually, a valid consent form should be drafted for that purpose.

11. Data Processing Agreement

Section 29 of the Act requires companies that act as data controllers to enter into data processing agreements with appropriate clauses whenever they contract a data processor to carry out the processing of personal data. The data processing agreement can either be a stand-alone document or have appropriate clauses inserted into a service-level agreement between the controller and the data processor.

12. Appointment of a Data Protection Officer

Section 32 of the Act requires a controller of major importance to designate a Data Protection Officer with expert knowledge of data protection law and practices, and the ability to carry out the tasks prescribed under the Act and other Data Protection Laws. Pursuant to this provision, companies that process data are mandated to appoint a Data Protection Officer.

13. Data Security

Section 24(f) and 39 of the Act enjoins companies that deal with data to implement technical mechanisms such as encryption, pseudonymization, anti-malware, firewall, etc. to ensure adequate protection of personal data from data breach. Therefore, the company should consider implementing internationally accepted standard controls for cybersecurity such as ISO 27100.

14. Data Retention

Companies that deal with data are not allowed to retain the data of a data subject longer than is necessary. A data retention policy and schedule should be maintained to ensure that personal data is deleted, anonymised or suppressed after an appropriate time unless a law requires that data be kept for a minimum time. The company should ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymized in accordance with the company's data retention guidelines.

15. Reporting of Personal Data Breach

The Act requires companies to report a personal data breach to the Commission within 72 hours of becoming aware of the data breach that is likely to result in a risk to the rights and freedoms of data subjects and to inform data subjects where the breach will result in a high risk to the right and freedom of data subjects. Therefore, in-scope companies should put procedures in place to deal with any suspected personal data breach, as well as to notify the data subject and the Commission where there is a data breach.

16. Feedback Mechanism

The Act enjoins companies to provide their contact and office address information in their privacy notice along with the contact information of the data protection officer[17]. At the same time, the Act requires the companies to inform the data subject that he/she has the right to lodge a complaint to the Commission[18]. Companies are therefore enjoined to ensure that their privacy notice contains the contact information of the companies' DPO and the contact of the Commission or link to their website as a best practice.

17. Policy Review

With the enactment of a new Act, companies are expected to take steps to review their policies and privacy framework to comply with the requirement of the Act. Therefore, companies are encouraged to review their policies and processing activities to fall in line with the provisions of the Act.

NEW CONCEPTS UNDER THE ACT

1. Scope of the Act

In terms of application, the scope of the Act is more elaborate and focuses more on the data controller and data processor and the location of the processing activities in order to determine its applicability, unlike the previous regime which focused its applicability on citizens and non-citizens. Consequently, the personal data of a citizen

[17] Section 27(1)(a) Nigeria Data Protection Act, 2023
[18] Section 27(1)(f) Nigeria Data Protection Act, 2023

of the Republic of Ghana who is resident in Ghana but has his/her personal data processed by a company in Nigeria will enjoy the protection of the Act[19].

2. Genetic and Biometric Data

The Act introduced and included genetic and biometric data as sensitive personal data. It is important to note that the Act defined biometric data but did not define genetic data. Biometric data are defined as personal data that results from specific technical processing relating to the physical, physiological, or behavioral characteristics of an individual, which allow or confirm the unique identification of that individual, including without limitation by physical measurements, facial images, blood typing, fingerprinting, retinal scanning, voice recognition, and deoxyribonucleic acid (DNA) analysis[20]. This provision is laudable as both genetic and biometric data could lead to social, religious, and political discrimination and require higher levels of protection.

3. Grounds for Processing Sensitive

The Act has expanded the grounds on which data controllers can rely to process sensitive personal data. Under the previous regime, data controllers could only rely on explicit consent to process sensitive personal data, however, the Act now provides for other grounds such as performance of employment contract, data subject's vital interest; legitimate activities of not-for-profit organization; exercise of legal defense; substantial public interest, medical care, public health; archiving, historical, statistical, or scientific research purposes[21]. These grounds will present more options for data controllers, remove the hardship presented by the provision of the previous regime and promote viable commercial activities in businesses involved in processing personal data.

4. Demonstration of Accountability (Documentation)

Under the NDPR, a data controller has a duty of care to ensure that the personal data of the data subject is protected. The Act has added an additional obligation on the controller to "demonstrate accountability"[22]. This means that it is not enough to comply with lawful processing and protection of personal data, but the controller must show such compliance. Therefore, data controllers must document their processing activities to show compliance. This documentation is achieved through a record of processing activities (RoPA).

5. Legitimate interest

[19] Section 2 (1)(a-c) Nigeria Data Protection Act, 2023
[20] Section 65 Nigerian Data Protection Act, 2023.
[21] Section 30 Nigeria Data Protection Act, 2023.
[22] Section 24(3) Nigeria Data Protection Act, 2023

The Act included legitimate interest as one of the lawful bases for processing personal data with certain conditions[23]. Prior to the enactment of this Act, there was unsettled controversy on whether NDPR provided for legitimate interest as a lawful basis. This is because while legitimate interest was patently omitted under the section for lawful basis[24], other provisions of NDPR and Implementation Framework referred to it[25]. This has now been settled by the Act with the provision of legitimate interest as one of the lawful bases for processing personal data.

6. Children's Personal Data

The provision of the Act requires companies involved in data processing to obtain the consent of the guardian or parent prior to processing a child's personal data. It further mandates the data controller to employ an "appropriate mechanism" to verify the age and consent obtained from a child[26].

Therefore, it will not be an excuse for a company to feign ignorance. For instance, if a child intentionally back dates his/her age and registers a social media account, without a data controller putting in place a mechanism that will ascertain the child's true age through a government-issued identification document and prevent such registration, the data controller will be liable. However, the provision above will not apply if the processing is necessary to protect the vital interest of a child or carried out for purposes of education, medical or social care or undertaken by a professional or similar service provider owing a duty of confidentiality. It will also not apply where the processing is necessary for proceedings before a court relating to a child[27].

7. Registration with the Commission

As stated, above section 44 of the Act requires data companies of major importance to register with the Commission within 6 months of the commencement of the Act (i.e., December 2023).

8. Data Controller or Processor of Major Importance

The Act introduced data controller and processor of major importance albeit without providing a clear meaning as to what constitutes data controller or processor of major importance. However, the Commission is empowered to prescribe what constitutes major importance. We are therefore looking forward to the guidelines of the Commission in this regard.

Conclusion

[23] Section 25 (10(b)(v), Nigeria Data Protection Act, 2023.
[24] Article 2.2 Nigeria Data Protection Regulation, 2019.
[25] Article 3.1(7)(d), 3.1(11)(d), 3.1(9) Nigeria Data Protection Regulation, 2019 and Paragraph 1.18 Audit Template Questionnaire.
[26] Section 31(1)(2)(3) Nigeria Data Protection Act, 2023
[27] Section 31(4) Nigeria Data Protection Act, 2023

Data controllers and data processors are encouraged to comply with the provisions of the Act to attract customers' trust and position themselves to attract competitive investors. Further, non-compliance may subject a data controller and data processor to reputational damage and penalty up ₦10,000,000 (Ten Million Naira only), and 2% of its annual gross revenue or ₦2,000,000 (Two Million Naira) and 2% of its annual gross revenue depending on whether the data controller and data processor are of major importance, among other punishment[28].

It is important to note that the Act did not repeal the provisions of the NDPR and the Implementation Framework in force prior to the Act[29]. Therefore, the provisions and obligations contained in these subsidiary legislation will remain in force except where it contradicts or conflicts with the provision of the Act or becomes repealed.

LAGOS
Plot 1B, Block 129,
Jide Sawyerr Drive,
Lekki Phase I
Lagos State, Nigeria

ABUJA
4th Floor, Abia House,
Plot 979, 1st Avenue,
Off Ahmadu Bello Way,
Central Business District,
Abuja FCT, Nigeria

Tel.: 0700 DOALAW (0700 362529)
Email: info@doa-law.com
www.doa-law.com