NIGERIA DATA PROTECTION ACT 2023

PART V

TONBOFA
Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE

INTRODUCTION

In the realm of data privacy, understanding the core principles of Personal Data processing is essential. these principles, as outlined in the Act, emphasize fairness, transparency, and accountability in handling Personal Data in Nigeria. The Act introduces key concepts like Data Privacy Impact Assessments("DPIA") and provides criteria for lawful data processing, ensuring that Data Subjects have control through consent. This article explores these principles, the responsibilities of Data Controllers and Processors, and their obligations to Data Subjects, reflecting Nigeria’s commitment to a secure and respectful data environment.

TONBOFA
Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE

PRINCIPLES OF PERSONAL DATA PROCESSING

1.1. Personal Data must be:

- Processed in a fair, lawful and transparent manner;
- Collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes;
- Adequate, relevant, and limited to the minimum necessary for the purposes for which the Personal Data was collected or further processed;
- Retained for not longer than is necessary to achieve the lawful basis for which the Personal Data was collected or further processed;
- Accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the Personal Data is collected or is further processed; and
- Processed in a manner that ensures appropriate security of Personal Data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.

1.2. In addition to the above principles, a Data Controller and Data Processor owes a duty of care to the Data Subject and must demonstrate accountability and use proper technical and organisational measures to ensure confidentiality, integrity, and availability of Personal Data.

1.3. Further Processing

Further processing of data is not permitted when done in any way incompatible with the principles spelt out under the Act. Under the NDPR, further processing of data may only be done for archiving, scientific research, historical research or statistical purposes for the public interest.

The Act expands on this provision and in addition to further processing for the purpose under the NDPR, provides for criteria to assess the compatibility of data for further processing. This includes;

- The relationship between the original purpose and the purpose of the intended further processing;
- The nature of the Personal Data concerned;
- The consequences of further processing;
- How the Personal Data has been collected; and
- The existence of appropriate safeguards.

TONBOFA Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE

LAWFUL BASIS FOR PERSONAL DATA PROCESSING

According to the Act, processing of Personal Data will be lawful where the Data Subject has given consent, and not withdrawn it, for the specific purpose(s) for which the data is to be processed; and where such processing is necessary; does not override the fundamental rights, freedoms and the interests of the Data Subject; and the Data Subject would have a reasonable expectation that the Personal Data would be processed in the manner envisaged.

Processing is deemed necessary:

- For the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject prior to entering into the contract
- For compliance with the legal obligation to which the Data Controller or Data Processor is subject,
- To protect the vital interest of the Data Subject or another person,
- For the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller or Data Processor , or
- for the purposes of the legitimate interests pursued by the Data Controller or Data Processor , or by a third party to whom the data is disclosed.

TONBOFA
Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE

CONSENT

Consent must be freely and intentionally given by the Data Subject, taking into account whether consent was given as a condition for the performance of a contract or provision of services for processing of Personal Data not necessary for the contract.

Consent may be provided in writing, orally or electronically. Silence or inactivity does not constitute consent.

The Data Subject can withdraw consent at any time and must be informed of his right to withdraw at any time. The burden of proof is on the Data Controller to prove that consent was properly given by the Data Subject in accordance with the provisions of the Act.

By virtue of section 31 of the Act, where the Data Subject is a Child or a person lacking the legal capacity to give consent, the consent of the parent or guardian shall be relied upon except where the processing is necessary to protect the interest of the Child or person lacking legal capacity to give consent or where the processing is to be carried out for educational, medical or social care purposes by a professional or service provide with a duty of confidentiality or where it is necessary for a court proceeding relating to the Child or person lacking legal capacity to give consent.

TONBOFA
Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE

PROVISION OF INFORMATION TO THE DATA SUBJECT

The Data Controller shall have a privacy policy, that's written clearly and easily accessible to the Data Subject and contains the following information:

- The identity, residence or place of business of the Data Controller
- means of communicating with the Data Controller or its representatives when necessary
- The lawful basis of processing, and the purpose for processing, the Personal Data
- The rights of the Data Subject
- The total period for which the Personal Data will be stored by the Data Controller or any Third-party
- The recipient or categories of recipients of the Personal Data
- The right to lodge a complaint with the Commission, where necessary; and
- The existence of automated decision-making, its significance, the consequence of such processing to the Data Subject and his right to challenge such processing

The Data Controller is not compelled to provide to the Data Subject the above information if it has already done so or if there would be a disproportionate effort or expense.

TONBOFA
Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE

INTRODUCTION OF DATA PRIVACY IMPACT ASSESSMENT

Another significant provision of the Act is the introduction of the concept of Data Privacy Impact Assessment ("DPIA"). It provides that a Data Controller shall prior to data processing conduct a DPIA where the processing of Personal Data may likely result in high risk to the rights and freedoms of the Data Subject by virtue of the nature, scope, context and purposes of processing. The Data Controller shall consult the Commission prior to processing if the impact assessment indicates that the processing of the data would result in a high risk to the rights and freedoms of the Data Subject.

The Commission may make regulations or issue directives with regard to the categories of processing and persons subject to the requirement for the conduct of a data privacy impact assessment.

A DPIA is a process designed to identify the risks and impact of the envisaged processing of Personal Data, and it comprises -

- A systematic description of the envisaged processing and its purpose, including the legitimate interest pursued by the Data Controller, Data Processor , or third party;
- An assessment of the necessity and proportionality of the processing in relation to the purposes for which the Personal Data would be processed;
- An assessment of the risks to the rights and freedoms of a Data Subject; and
- The measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of Personal Data, taking into account the rights and legitimate interests of a Data Subject and other persons concerned.

TONBOFA
Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE

OBLIGATIONS ON ENGAGEMENT OF DATA PROCESSOR

The Act also dictates certain measures which should be included in a written agreement between the Data Controllers and the Data Processor , or between Data Processors.

These measures include that the engaged Data Processor :

- complies with the principles and obligations set out in this Act as applicable to the Data Controller;
- assists the Data Controller or Data Processor , as the case may be, by the use of appropriate technical and organisational measures, in the fulfilment of the Data Controller's obligations to honour the rights of a Data Subject;
- implements appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of Personal Data as required in Part VII of the Act;
- provides the Data Controller or engaging Data Processor , where applicable, with information reasonably required to comply and demonstrate compliance with this Act; and
- notifies the Data Controller or engaging Data Processor , where applicable, when a new Data Processor is engaged.

PROCESSING OF SENSITIVE PERSONAL DATA

The Act defines “Sensitive Personal Data” as data relating to an individual’s genetic/biometric data, race or ethnic origin, religious or similar beliefs, health status, sex life, political opinions or affiliations, trade union memberships, or other information prescribed by the Commission.

This definition updates the meaning under the NDPR, replacing “sexual orientation” with “sex life” and while it does not include the individual’s criminal record in the definition, it gives the Commission the liberty to prescribe other classes of information in the future as Sensitive Personal Data.

The Act provides certain circumstances where sensitive Personal Data shall not be processed. Some of these circumstances include where the Data Subject has given consent and not withdrawn same; the processing is necessary for the Data Controller to perform its obligations or exercising the rights of the Data Subject under employment laws, social security laws or other similar laws; the processing is necessary where Data Subject legally cannot give consent to protect the vital interest of Data Subject or another person; or where the processing is necessary for the establishment, exercise or defence of a legal claim, obtaining legal advice, or conduct of a legal proceeding.

The Commission may make further regulations and directives on further categories of Sensitive Personal Data, grounds for processing such data and safeguards which may apply, having regard to the significant harm that such processing could cause, the reasonable expectation of confidentiality attached to such data and adequacy of protection afforded to Personal Data generally.

TONBOFA
Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE

DATA PROTECTION COMPLIANCE

To ensure that a Data Controller complies with the provisions of the Act, it is mandated to engage a Data Protection Officer (DPO), who might already be an employee of the Data Controller, with expert knowledge of data protection laws and practices to advise the Data Controller or Data Processor or its employees; monitor with the provisions of the Act, the policies of the Data Controller/processor and other regulations of the Commission; and act as a contact point between the Data Controller/Processor and the Commission.

The Act also grants the Commission power to license any person, with requisite level of expertise, to monitor, audit and report on the compliance by Data Controllers/Processors with the provisions of the Act and other regulations or guidelines issued by the Commission.

CONCLUSION

In conclusion, the Principles of Personal Data Processing introduced in the Act serve as a foundational guide for ethical data handling in Nigeria. With an emphasis on fairness, transparency, and accountability, the Act not only aligns with international data protection standards but also sets a clear path for responsible data processing in the digital age. By introducing innovative concepts such as Data Privacy Impact Assessments and safeguarding individual consent, Nigeria takes a significant stride towards a robust, secure, and privacy-respecting data landscape. These principles are not just a legal framework; they are a testament to the nation's commitment to protecting the rights and privacy of its citizens in an increasingly data-driven world.

THANK YOU

LAWYERS@TONBOFA.COM

Follow us for more on our website below

WWW.TONBOFA.COM

TONBOFA
Law Practice
CONSULTING | LEGAL ADVISORY | LEGAL REPRESENTATIVE