ENDOXA

REGULATORY UPDATE NO. 2 OF 2023

PERSONAL DATA PROTECTION ACT, 2022

ENDOXA

WHAT YOU NEED TO DO?

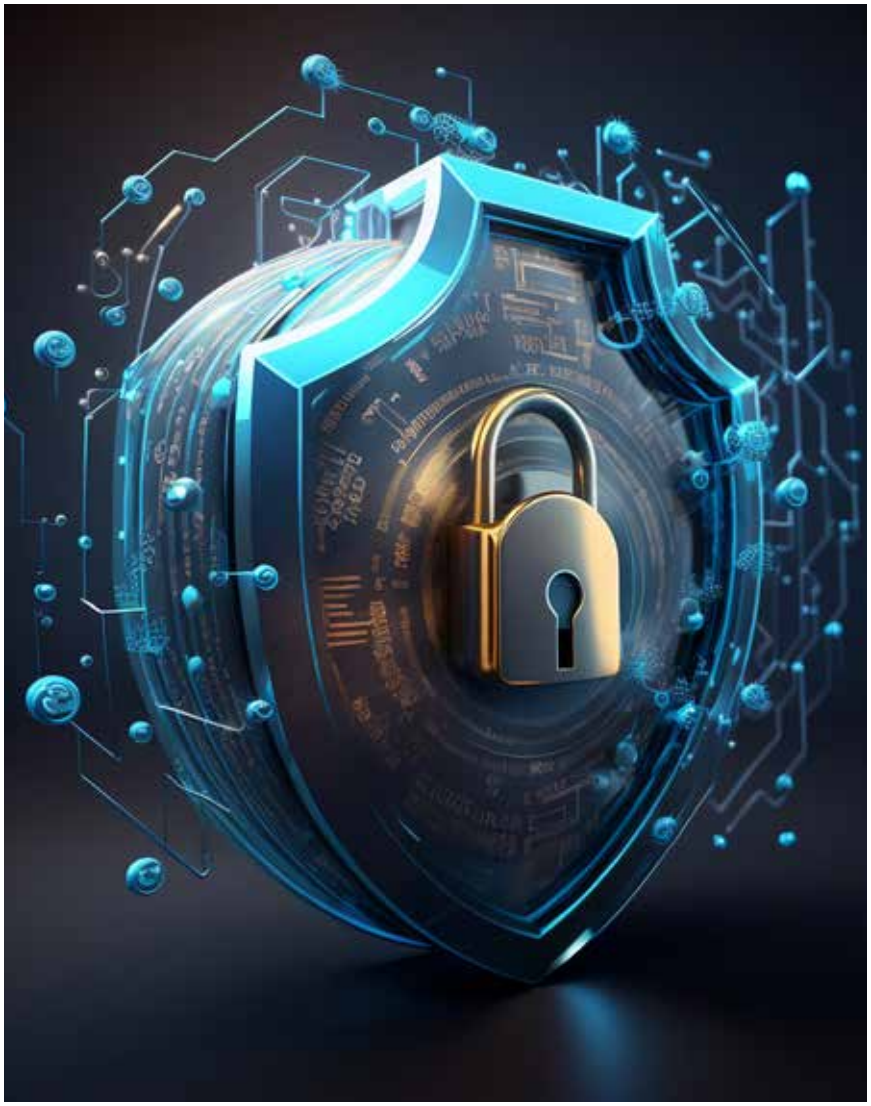
Recently, our firm, Endoxa Law, is receiving a lot of queries from clients seeking to understand and implement the requirements in the Personal Data Protection Act, 2022. Whilst the Minister of Information, Communication and Information Technology has not yet published the notice making this law operational, we are advising clients to commence the preparatory work for their business to be compliant. The starting point should be the process of amending agreements to incorporate data protection and information security provisions. However, there is a lot more that needs to be done.

In this article, we consider why and how our clients should start preparing for the arrival of the Personal Data Protection Act, 2022, and how this Act will become a game changer.

ENDOXA

What is PDPA?

Interestingly, a few months before the European Union voted to adopt the General Data Protection Regulations (GDPR) and before South Africa adopted the Protection of Personal Information Act (POPIA) in November 2013, the Tanzanian Ministry of Communication, Science And Technology sponsored had already identified the need for a conducive legislative framework that protects personal data and sponsored the data protection and privacy bill, 2013. on the 2nd December 2022, almost ten (10) years later, the parliament of Tanzania passed the Personal Data Protection Act, Act No. 11 of 2022 (PDPA). It will become operational when the Minister publishes a notice of the commencement date in the government gazette. In the meantime, clients are advised to take the necessary steps to prepare their businesses to comply with the key requirements of the PDPA.



ENDOXA

What is protected?

Personal information/data: means information regarding an individual recognized in any manner which includes;

- personal information relating to an individual's race, national or ethnic origin, religion, age or marital status;
- personal information regarding education, medical history, criminal or employment history;
- any identification number, mark or other special form that identifies an individual;
- the address, fingerprints or blood group of the individual;
- the name of an individual that appears in the personal information of another person related to him or where the disclosure of that name will reveal the personal information of the person;

Sensitive Personal Information: includes the following;

- genetic information, information concerning children, information concerning errors, financial transactions of an individual or security measures, biometric information;
- if processed, is personal information indicating racial or ethnic origin, political ideology, religious or philosophical beliefs, affiliation, trade union membership, gender and medical records or sexual relationships; and
- any personal information that according to the laws of the country is considered to have a significant impact on the rights and interests of the subject of the information.
- information sent to the collector of personal information by a person, which it is clear that the information is personal or confidential, and responses to the information may reveal the content of the previous information, and the view or opinion of any other person about the subject of the information.

Who is affected?

Collector: means any person, private or public institution which on its own or with other person or institution decides the purposes and means of processing personal information/data and where the purposes and means of processing data are stipulated under the law and will include their representatives.

Data Protection Officer: means the person appointed by a collector or processor who is responsible for ensuring regulatory and security measures are taken by the company to protect the personal information collected or processed.

Data Subject: the subject of personal information processed in accordance with the law.

Processor: any person, private or public institution which processes personal information/ data for or on behalf of data collector with the collector's instructions with exception of those under the authority of the data collector who are allowed to process the personal information/data and will include their representatives.

Receiver: any person, private or public institution or any other person who receives personal information/data from the collector.

ENDOXA

Key duties of Collectors and Processors

1. Duty of Collector and Processors to appoint a personal information protection officer who will ensure that regulatory and security measures are taken to protect the personal information collected or processed.
2. Duty to register with the Data Protection Commission and obtain a certificate which is valid for five years. Renewal applications must be lodged at least three (3) months from expiry.
3. Recognition of 'legitimate purposes' as the lawful basis for collection of data.
4. The information must be collected directly from the Data Subject.
5. Duty to ensure the Data Subject
   a. understands the purpose of collecting personal information;
   b. is aware that the collection of personal information is for an authorized purpose; and
   c. knows the intended recipients of the personal information.
6. Duty not to use personal information in the existing environment without taking steps to ensure that the information is complete, accurate, consistent with the content and not misleading.
7. Duty to use personal information only for the purpose it was collected. Exceptions where the collector can use the information collected for other purpose if:
   a. Where the Data Subject has authorized the use of personal information for that purpose;
   b. the use of personal information for that purpose is authorized or required by law;
   c. the purpose for which personal information has been used is directly related to the purpose of collecting that information;
   d. personal information is used in such a way that the subject is not identified or for statistical or research purposes and will not be published in a manner that can identify the subject;
   e. the collector believes for reasonable reasons that the use of personal information for that other purpose is necessary to prevent or reduce harm to the life or health of the person concerned or another person, or to the health or safety of society or the use of personal information for other purposes is important in compliance with the law.
8. Duty to avoid disclosure of personal information to a person other than the subject of the information, except for the circumstances specified in under the law (as listed in clause 6 above).

9. Duty to protect personal information by taking the necessary security measures for the safety of such information against careless loss or destruction, conversion, access or processing of personal information without authorization by considering both technological change and the costs of implementing such measures as well as the type of personal information that should be protected and the harm that may occur to the subject of the information.
10. Duty to notify the Commission of any breaches of security pertaining to personal information.
11. Duty to obtain prior 'written' informed consent from the Data Subject before processing personal information.
12. Duty to inform the Data Subjects of their rights including:
    a. Right to be informed if personal information is being processed by that collector or another collector on behalf of that collector;
    b. Right to be provided by the collector with details of personal information about him, the purpose of the processing and recipients or groups of recipients to whom or who may be given such information;
    c. where the automatic processing of personal information for the purpose of evaluating matters concerning him, has been used or may be used as the sole basis for decisions having a significant impact on him, to be informed by the collector about the reasons used to reach that decision.
13. The collector or his representative is required to ensure the decision which has a significant impact on the Data Subject should not rely solely on automatic processing, and if it does, the Collector to inform the Data Subject as soon as possible if there is no prior consent
14. Duty to modify, block, delete or destroy wrong personal information at the request Commission and application of a Data Subject to the commission and to inform the third party who received the relevant personal information about the modification, blocking, updating, deletion or destruction of such information.
15. Generally, Collectors and Processors must ensure personal information:
    - is processed lawfully, fairly and transparently;
    - is collected for a specific, specified and legitimate purpose, and such information will not continue to be processed in a manner different from the specified purpose;
    - is sufficient and necessary for the purposes of the processing as intended;
    - is correct and where necessary, is improved by taking all necessary measures to ensure that incorrect personal information is deleted or corrected without delay;
    - is stored in a manner that allows the identification of the subject of the information for a period not exceeding that required for the purpose of processing the relevant personal information;

- is processed in accordance with the rights of the data subject;
- is processed in a manner that will ensure the security of personal information, including protection against unauthorized or illegal processing and against any loss, damage or harm, using appropriate technical or administrative measures; and
- is not exported outside the borders of the country contrary to the provisions of the PDPA specified below.

Conditions for cross border transfers of personal information

The PDPA sets a clear regime for cross border transfers of personal information with a more relaxed regime for transfers for countries with adequate protection of personal information versus countries with an inadequate regime for protection of personal information.

What should be done?

Why act now?

To avoid penalties for non-compliance in the future. Such penalties include:

- Loss of regulatory licence to collect or process personal information
- Penalties for the criminal offence of providing false or misleading information during registration includes imprisonment of up to five years and seizure of equipment.
- Compensation to be paid to the Data Subject of amounts to be determined by the Minister.

What should be done?

To avoid delays in collecting and processing data due to the need for consent from Data Subjects, Endoxa Law is recommending all our clients should include appropriate data protection wordings and information security policy requirement in all their legal agreements. This includes, but is not limited to, the following agreements:

- operational contracts
- commercial contracts
- technical services agreement
- credit agreements

Endoxa has established a data protection team to assist clients with the review and amendment of existing agreements and standard templates to cater for the requirements of PDPA. Once the PDPA is operational, the team will assist with the registration of clients as data Collectors or data Processors as well as the registration of the Data Protection Officers. If requested by clients, we will arrange for appropriate sections of the PDPA to be translated from Swahili to English.

Should you want any assistance from our team please send an email to: info@endoxagroup.co.tz

ENDOXA

ENDOXA Law
15 Tunisia Road, Ada Estate, Dar Es Salaam, Tanzania/+255767211883/www.endoxagroup.co.tz
/Email: info@endoxagroup.co.tz