THE DATA PROTECTION ACT AND ITS IMPLICATION ON BUSINESS IN TANZANIA.

By Sunday Ndamugoba and Lucas Maduhu

Introduction

The Personal Data Protection Act No. 11 of 2022 (the **Act**) was passed on 1st November 2022 as a recognition of the right to privacy and personal security enshrined under Article 16 of the Constitution of the United Republic of Tanzania, 1977. The Act sets minimum requirements for the collection and processing of personal data in Tanzania.

Application of the Act

The Act applies to both public and private institutions with the responsibility to collect and process personal data in Tanzania. Protection of personal data existed before the enactment of the Act, however, the Act comes in to strengthen such protection and provide specific remedies for breaches in relation to personal data.

Objectives of the Act

The Act was prepared in order to ensure that the collection and processing of personal data is strictly controlled. This is achieved through establishing legal and institutional arrangements for the protection of such information. According to Section 4 of the Act, data collectors and processors shall ensure that personal information:

- Is processed lawfully, fairly and transparently;
- Is collected for a specified legitimate purpose and not processed for any other purpose;
- Is sufficient for the purpose of processing in accordance with the intended purpose;
- Is correct and where necessary improved by taking all necessary measures to ensure that the incorrect information is deleted and replaced without delay;
- Is stored in a manner which allows identification of the data subject for a period not exceeding that which is necessary;

- Is collected in accordance with the rights of the data subject;
- Is processed in a manner that will safeguard its security; and
- Is not transferred outside the United Republic of Tanzania contrary to the provisions of the Act.

Data Protection and Businesses

The Personal Data Protection Act No. 11 of 2022 applies to any information an organisation keeps on staff, customers or account holders and will likely inform many elements of business operations, from recruitment, managing staff records, marketing or even the collection of CCTV footage.

Whilst there may be additional protections that need to be applied to special category information, personal data of all kinds must be adequately secured, accurate and up to date, whilst satisfying the rights of subjects.

Depending on the types of storage, processing or transportation that your business conducts upon personal data, at least some methods of encryption, segmentation and pseudonymisation will likely need to be applied, and specialist expertise should be sought if you're unsure about any technical elements of these processes.

Data Protection Authorities

Section 6 of the Act establishes a Personal Data Protection Commission (the **Commission**) which is a body corporate with perpetual succession and a common seal. The Commission is tasked with various functions which include:

- monitoring the compliance of data collectors and processors with the Act;
- registration of data collectors and processors;
- receiving, investigating and handling complaints on the breach of data protection and the right to privacy; and
- researching and monitoring technological development in relation to data processing.

Registration of Data Collectors and Processors

Section 14 of the Act provides a strict requirement for any person who intends to collect or process data in Tanzania to be registered by the Commission. Registration is initiated through an application made to the Commission which will either accept or reject the application. Upon acceptance, the Commission will issue a certificate of registration and

where rejected, the Commission will provide its reasons for the decision in writing.

An issued certificate of registration shall be valid for a period of five (5) years from the date of issuance. The Act directs that all applications for renewal be made three months before the expiry of the registration period. The Act further provides a leeway for the Commission to cancel an issued certificate of registration.

Data Collection, Use, Disclosure and Retention

Section 22 of the Act directs that personal information be collected where necessary and for a legitimate purpose. To ensure the accuracy of the information, the Act places a duty on data collectors to take necessary steps to confirm that the data collected is complete, correct and consistent with the content for which it was collected. Such steps are necessitated prior to using the collected data.

According to the Act, data collected may only be disclosed under the following circumstances:

- Where the data subject has consented to such disclosure;
- Where authorised or required by law;
- Where disclosure is directly related to the purpose for which such data was collected;
- Where such disclosure would preserve health or reduce harm to another person or society; and
- Where disclosure is necessary in compliance with the law.

As per Section 25(2) of the Act, disclosure of information may also be permitted where:

- The data subject is not identified; or
- For statistical or research purposes, where it is guaranteed that such data will not be published in a manner that will identify the data subject.

Additionally, Section 27 of the Act requires data collectors to appoint a Personal Data Protection Personnel/Officer, and maintain a proper security system dedicated to ensuring that the data collected is not destructed, converted, accessed or processed in any way without authorisation.

Data Transfer

Section 31 of the Act allows the transfer of personal data to other jurisdictions, provided that such jurisdictions have a reliable legal system for the protection of personal data, and

the said transfer is necessary for a legitimate or public interest. Please note that the Commission may restrict the transfer of personal data to other countries in accordance with the Act. In some instances, personal data may be transferred to a receiving country with no specific legal protection on personal data but has guaranteed protection of such data.

Rights of Data Subject

As a guarantee to the protection of personal data, Part VI of the Act vests the following rights upon a data subject:

- Right to be informed of data collection and processing as well as the purpose involved;
- Right to access the data collected and processed;
- Right to object to the processing of personal data collected where such processing will lead to adverse impacts;
- Right to rectify personal data to ensure its accuracy;
- Right not to be subject to automated decision-making. A data subject has the right to instruct that decisions made by data collectors and processors on their behalf should not be arrived at, solely based on automated processing; and
- Right to compensation.

Complaints and Penalties

According to Section 39 of the Act, a person may file a complaint against a data collector or processor who has violated the principles of personal data protection. Please note that such complaints are submitted to the Commission. The Commission will initiate a confidential investigation where satisfied that there are fundamental reasons to investigate. Such investigation will be conducted and concluded within 90 days, however, under certain circumstances, the Commission may extend such period.

Where it is determined that there has been a violation in the provisions of the Act, the Commission may issue an enforcement notice directing the respective person to remedy such violation within a certain period. Furthermore, the Commission may issue a notice of penalty where the respective party has failed to remedy the violation within the given period.

According to the Act, unconsented disclosure of personal data by an individual shall constitute an offence punishable by a fine of not less than TZS 100,000 (approximately USD 43) and not more than TZS 20,000,000 (approximately USD 8,600) or to imprisonment for a term not exceeding ten years. In some instances, both a fine and imprisonment may be

imposed.

With regards to a body corporate, the Act imposes a fine of not less than TZS 1,000,000 (approximately USD 430) and not more than TZS 5,000,000,000 (approximately USD 2,127,700) for unconsented disclosure of personal data.

The Act further establishes an offence of unlawful destruction, deletion, concealment or conversion of personal data. This offence is punishable by a fine of not less than TZS 100,000 (approximately USD 43) and not more than TZS 10,000,000 (approximately USD 4,300) or to imprisonment for a term not exceeding five years. Both a fine and imprisonment may be imposed in some instances.

Where an offence is committed by a body corporate, the Act poses a direct liability on all officers who intentionally authorised or allowed the commission of such an offence.

Additionally, the Act stipulates a general fine of not less than TZS 100,000 (approximately USD 43) and not more than TZS 5,000,000 (approximately USD 2,200) or imprisonment for a term not exceeding five years, or to both, a fine and imprisonment. This provision will apply where the Act does not specifically provide punishment for an offence.

Businesses Actions Going Forward

1. ***Reduction in Data Collection***

Most for-profit businesses gather and store data in order to develop their company and better understand their target market. Unfortunately, countless data breaches have proven that storing data can be a big liability. Businesses are becoming more conscious of the risks associated with excessive data collection, whether it be consumer or staff data. As a result, and with the law it is best to start to revise consumer and staff data collection procedures. It is best to only retain critical data to limit possible exposure and liability concerns.

2. ***Risk Management for Third-Parties***

Looking towards the future, businesses will heavily emphasize third-party risk management, risk assessment, and compliance. New requirements under the law include contractual safeguards, sufficient data protection, and proof of compliance. This means that organizations will have to spend more time evaluating third-party partners to protect

themselves from possible threats.

Rather than using third-party data processors, companies are advised to keep everything in-house to avoid stolen data. Businesses have limited control over how third-party organizations deal with data and privacy. It's very difficult to ensure that a third party is compliant with regulations

3. ***A Shift in Roles and Reporting***

Companies will inevitably depend on internal data managers as more privacy, and data-related rules and regulations are implemented. In terms of data collecting, Personal Data Protection Personnel/Officers are vital in keeping organizations compliant.

4. ***Building Trust through Data Privacy***

While there are many new regulations and standards in data privacy, they mostly follow these guidelines:

- Organizations should alert consumers about data collection, processing, and sharing.
- Customers should be able to request access to their personal data at any time.
- Companies shouldn't collect data without consent.
- Customers should be able to request that their personal data be removed.
- Consumers should be able to fix personal data mistakes.
- Organizations should protect personal data with data security solutions.

Key Concerns about the law

There are however some unclear provisions which perhaps will be addressed in the future for example Section 35 prohibits the processing of personal data for direct commercial advertising purposes. Despite the prohibition, it still remains unclear whether the section data handlers can trade the personal data of their data subjects.

The act also falls short when it comes to the security breach notification front. Procedures for handling data breaches ought to be outlined in the Data Protection Regulation, in order to compel data handlers to give data subjects advance notice of any security breaches involving their personal information, its effects, and the remedial action is taken. The obligation for data breach notification would be greatly strengthened by a directive for data

processors and collectors to notify affected data subjects within a stipulated time of becoming aware of data breaches.

Part five of the act addresses data transfer, but the clause is opaque on the aspect of data subjects granting their consent to bodies that collect, process, store, or use personal data outside Tanzania's borders. As data subjects have not been accorded the "power of consent," it means that their data may be prone to misuse.

Part six of the act is ambiguous. Section 34 (4), for example, gives full legal rights to an heir apparent, meaning that they could consent to the processing of private information on behalf of any other party not capable of granting such consent. It however lacks a legal interpretation rationale, as it does not clearly spell out which "party" — whether alive, incapacitated, and/or deceased. This section may be prone to abuse, as an heir may not meet the legal threshold to consent on behalf of someone else due to reasons such as being underage, coercion, and/or other technicalities.

Conclusion

This Act welcomes regulatory development and will lead to a higher level of personal data protection in Tanzania's growing digital economy. The Act is more closely aligned with international data privacy standards.

After implementing the above guidelines businesses are still able to understand their customer's needs. They can also still send extremely relevant and engaging customized messages via sophisticated audience-based marketing. As a result, many businesses are embracing the changes brought on by increasing data privacy and are implementing strategies to reduce potential liabilities. This they hope will allow them to build trust, and stay ahead of the curve by implementing solutions and systems that enable the use of consumer data while being transparent.

In the changing landscape of data privacy, it has become very crucial that businesses implement strong security to protect the data they collect.

Click here SHERIA YA ULINZI WA TAARIFA BINAFSI to download The Personal Data Protection Act No. 11 of 2022 (the **Act**) of Tanzania in swahili

Disclaimer!

This brief on the Data Protection Act has been prepared for informational purposes only and does not constitute legal advice. It is intended to provide a general overview of the Act, and should not be relied upon as a substitute for legal advice specific to your individual circumstances. Before taking any action based on the information provided in this brief, we recommend that you seek the advice of qualified lawyers who can provide legal advice specific to your individual circumstances. If you require legal advice on the Act or related matters, please feel free to engage our firm to provide you with the necessary legal assistance.