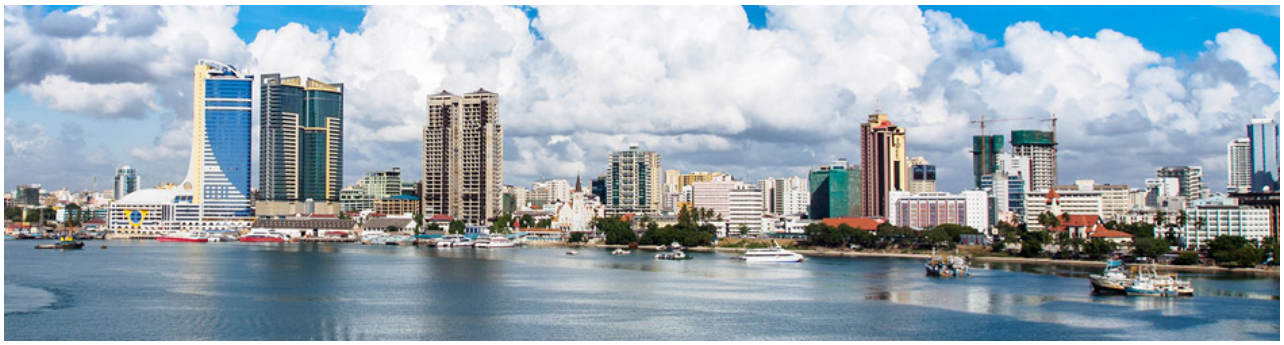
DATA PROTECTION LAWS OF THE WORLD

Tanzania

DLA PIPER

TANZANIA



Last modified 25 January 2024

LAW

On 1 May 2023, the Personal Data Protection Act, 2022 (“**PDPA**”) came into force. The PDPA provides for matters relating to protection of personal data and establishes the principles guiding and conditions for collection and processing of personal data. The principles guiding protection of personal data are provided under section 5 of the PDPA, which include:

i. personal data must be processed lawfully, fairly, in a transparent manner ensuring its security and in accordance with the right to privacy of the data subject;
ii. personal data must be collected for explicit, specified, and legitimate purposes and not further processed contrary to those purposes;
iii. personal data must be accurate and kept up to date and corrected or deleted without delay when inaccurate;
iv. personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
v. personal data must be kept in a form which identifies the data subjects for longer than is necessary for the purposes for which it was processed; and
vi. personal data must not be transferred outside Tanzania contrary to the provisions of the DPA.

In addition, the PDPA provides for the following, among other things:

- Part 2 establishes the Personal Data Protection Commission (“**Commission**”) which will be responsible to ensure implementation of the provisions of the Act. The Commission will also be responsible for registration of data processors and data collectors in Tanzania;
- Part 3 provides for registration of the controllers and processors of personal data;
- Part 4 provides for principles relating to collection, use, disclosure and storage of personal data;
- Part 5 provides for transfer of personal data outside Tanzania; and
- Part 6 provides for rights of the data subjects.

The Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 (“**PDPA Regulations** ”) made under the PDPA also came into effect on 4 July 2023 and make provisions for matters connected with the PDPA.

The PDPA and its Regulations are the principal data protection laws, supplementing other laws providing for data protection in Tanzania, including the Constitution of the United Republic of Tanzania, 1977 (“**Constitution**”) and other sector specific legislations, for instance the Electronic and Postal Communications Act, 2010 (“**EPOCA**”) and its regulations applicable to the electronic and postal communication sector and the National Payment System Act, 2015 (“ **NPS Act**”) and the Bank of Tanzania (Financial Consumer Protection) Regulations, 2019 applicable to the financial services sector.

DEFINITIONS

Definition of Personal Data

The PDPA defines “personal data” as data about an identified or identifiable person that is recorded in any form, including such person’s:

- personal data relating to the race, national or ethnic origin, religion, age or marital status;
- personal data relating to the education, medical history, criminal or employment history;
- identification number, symbol or other assigned particular;
- address, fingerprints, or blood type;
- name appearing in the personal data of another person or where the disclosure of that name itself will reveal the personal data of that person; and
- correspondence sent to a data collector by the data subject that is explicitly or implicitly of a private or confidential nature, and responses to such correspondence that would reveal the personal data about the individual.[1]

Definition of Sensitive Personal Data

The PDPA defines “sensitive personal data” to include the following information:

- genetic data, data related to children, data related to offences, financial transactions of an individual, security measures or biometric data;
- if processed for what they reveal, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade union membership, gender and data concerning health or sexual life; and
- any personal data which according to the laws of the country is considered to present a major risk to the rights and interests of the data subject.[2]

1: Section 3 of the DPA

2: Ibid

NATIONAL DATA PROTECTION AUTHORITY

The PDPA provides for establishment of the Commission which will be responsible for monitoring and implementation of the provisions of PDPA in Tanzania. The Commission is yet to be established, but its functions are currently handled under the Ministry of Information, Communication, and Information Technology.

REGISTRATION

Every person collecting or processing personal data must be registered with the Commission.[1] Registration is valid for 5 years.[2]

1: Section 14 of the DPA
2: Section 16 of the DPA

DATA PROTECTION OFFICERS

Data controllers or processors must appoint a data protection officer whose role is to ensure that the control and security measures are in place to protect personal data that is collected or processed.[1] The data protection officer must, among other things, also ensure compliance of the PDPA and its regulations in the processing of the personal data by the data controller or processor, handle applications or complaints made by data subjects, their representatives or any other person to the data controller or processor in relation to the collection or processing of personal data and prepare and submit quarterly compliance reports to the Commission.[2]

1: Section 27(3) of the DPA

2: Regulation 32 of the PDPA Regulations

COLLECTION & PROCESSING

The PDPA requires the data controllers to collect personal data directly from the data subject concerned.[1] The exception is where:

- the personal data is already in the public domain;
- the data subject has consented to the collection of his personal data from another person;
- compliance is not reasonably practicable in the current circumstances;
- non-compliance is necessary for compliance with other written laws; or
- compliance would prejudice the lawful purpose for which the collection is sought.

Prior to collecting personal data, the controller must ensure that the data subject is aware:

- of the purpose for which the personal data is being collected;
- of the fact that the collection of personal data is for authorised purposes; and
- any intended recipients of the personal data.[2]

Further, the controller or processor must ensure the data subject understands what they have consented to and must be afforded a simplified means to withdraw their consent.[3]

Personal data collected must only be used for the intended purpose.[4] Where a data controller collects personal data for any particular purpose, he cannot use such data for a different purpose unless:

- the data subject has consented to the use of his personal data for such purpose;
- the use of the data for such purpose is authorised or required by law;
- there is a direct correlation between the purpose for which the personal data is used and that for which the data was collected;
- the information is used in a manner which does not identify the data subject or for statistical or research purposes and is not published in a manner that could reasonably be expected to identify the data subject; and
- the data controller believes on reasonable grounds that the use of such personal data for the other purpose is necessary to prevent or lessen a serious and imminent threat to the health or life of the data subject or another person or to public health or safety; or
- the use of such personal data for that other purpose is necessary for complying with the law.[5]

1: Section 23(1) of the DPA
2: Section 23(2) of the DPA
3: Regulation 25(d) of the PDPA Regulations
4: Section 25(1) of the PDPA
5: Section 25(2) of the PDPA and regulation 26 of the PDPA Regulations

TRANSFER

The PDPA permits the transfer of personal data outside Tanzania only on the following circumstances:

- to a country that has a legal framework that provides for adequate personal data protection (i.e. essentially equivalent levels of protection to that within Tanzania) provided the recipient has established that:

1. such personal data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of a data controller; or
2. the importance of the transfer and there is no reason to assume that the subject's legitimate interests may be prejudiced by the transfer or the processing in the recipient country.[1]

The data controller must carry out a provisional evaluation on the need to transfer such personal data[2] and ensure the recipient of the data only processes the relevant information in the data and for the purpose for which the data was transferred.[3] The recipient of the data must also ensure that the necessity for the transfer of the personal data can be subsequently verified:[4]

- to any other country with appropriate safeguards on the security and protection of personal data provided the data is transferred solely to permit processing authorised to be undertaken by the controller;[5]
- to a country which does not have the adequate level of protection provided the transfer is in accordance with specifications issued by the Minister responsible for Information, Communication and Information Technology, the data subject has consented to such transfer and the transfer is necessary for:
    - the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken at the request of the data subject;
    - conclusion or performance of a contract concluded or to be concluded the controller and another person in the interest of the data subject;
    - or legally required on public interest grounds or the institution, trial defence of a legal claim;
    - protecting the legitimate interests of the data subject; and
    - the transfer is made in accordance with the law and is aimed to provide information to the public and is open for public consultation in general or by anyone who can demonstrate a legitimate interest, to submit their opinion in accordance with a procedure laid down by law.[6]

Prior to the transfer of personal data outside Tanzania, the data controller or processor must apply for and obtain a permit from the Commission.[7] The application is made using a prescribed form which must be accompanied with proof that:

- the recipient country has ratified an international agreement providing requirements for the protection of personal data;
- there is an agreement between Tanzania and the recipient country regarding the protection of personal data; or
- there is a contractual agreement between the person requesting the personal data and the recipient of the personal data who is outside Tanzania.[8]

1: Section 31(2) of the DPA
2: Section 31(3) of the DPA
3: Section 31(5) of the DPA
4: Section 31(4) of the PDPA
5: Section 32(1) of the PDPA
6: Section 32(4) of the PDPA
7: Regulation 20(1) of the PDPA Regulations
8: Regulation 20(3) of the PDPA Regulations.

SECURITY

The PDPA requires data controllers and their representatives to safeguard personal data by taking necessary security measures for the safeguard of such information against any negligent loss or unauthorised destruction, modification, disclosure, access or processing of personal data.[1]

The security measures that a data collector employs must ensure the required level of security by taking into account the following:

a. the state of technological advancement and the costs of implementing such measures; and
b. the nature of personal data that should be protected and the potential risks to the data subject;[2]

Data controllers are also required to appoint a personal data protection officer (refer to above).[3]

Any processing activity by a data processor must be governed by a contract that will specify the relationship between the processor and the controller in such a way that ensures the data processor will act under the instructions of the data controller and that the data processor will be responsible for ensuring compliance with the security standards provided under the PDPA.[4]

1: Section 27(1) of the DPA
2: Section 27(2)(a) and (b) of the DPA
3: Section 27(3) of the DPA
4: Section 27(4) of the DPA

BREACH NOTIFICATION

Data controllers must promptly notify any personal data security breach to the Commission. The breaches notifiable are any security breaches which affect personal data being processed on behalf of the data controller.[1]

Mandatory breach notification

As advised above, it is mandatory for every data controller to, promptly, notify the Commission of any breach of security that may affect personal data which is being processed on their behalf.

1: Section 27(5) of the DPA

ENFORCEMENT

The Commission established under the PDPA is mandated to ensure the implementation and enforcement of the provisions of the PDPA. The Commission has investigative and corrective powers including to:

- receive, investigate and handle complaints related to alleged contraventions of personal data and privacy of persons; and
- investigate and take necessary steps against anything it considers affects the protection of personal data and infringes privacy of individuals.[1]

The Commission is empowered to issue an enforcement notice on any person if satisfied that that such person has failed to comply with the provisions of the PDPA. Through this notice, the Commission will specify the provision of the Act which have been contravened, the steps which must be taken remedy or eliminate the infringement, the period within which such measures must be implemented (which cannot be less than 21 days), and any right to appeal.[2]

Where the person fails to comply with the enforcement notice and the Commission is satisfied to that effect, the Commission can issue a penalty notice requiring the person to pay fine to be specified in the notice. In determining whether to give a penalty notice and the fine payable, the Commission is required to consider the following:

a. the nature, gravity and duration of the infringement;
b. the intentional or negligent character of the infringement;
c. any measures taken by the data controller or processor to mitigate the damage or distress suffered by data subjects, including technical and administrative / organizational measures;
d. any previous infringements by the data controller or data processor;
e. the degree of co-operation with the Commission, in order to remedy the infringement and mitigate its possible adverse effects;
f. the categories of personal data affected by the infringement;

g. the manner in which the infringement became known to the Commission, including whether the data controller or processor notified the Commissioner of the infringement;
h. the extent to which the data controller or processor had complied with previous enforcement or penalty notices;
i. adherence to approved codes of ethics or terms and conditions of registration;
j. whether a penalty would be effective; and
k. any other aggravating or mitigating factors applicable to the case, including financial benefits gained, or losses suffered, as a result of the infringement (whether directly or indirectly).

The maximum penalty which the Commission may issue in the enforcement notice is Tanzania Shillings One Hundred Million (TZS 100,000,000, approx. US$ 430,000).[3]

The Commission may also direct the controller or processor to pay the affected data subject compensation for infringement of the PDPA and there is no ceiling on the amount of compensation which the Commission can award.[4]

Disclosure of personal data without lawful excuse (including obtaining such data or offering such data for sale) is also a criminal offense which on conviction carries a fine and / or imprisonment. For individuals, the minimum fine for a violation is Tanzania Shillings One Hundred Thousand (TZS 100,000, approx. US$43) and the maximum is Tanzania Shillings Twenty Million (TZS 20,000,000, approx. US$ 8,600).

The maximum term an individual may be sentenced for violating a provision under the PDPA is ten (10) years. If found in violation of the PDPA, an individual may be required to both pay a fine and serve a sentence.[5]

For a company or corporation, the minimum fine for a violation is Tanzania Shillings One Million (TZS 1,000,000, approx. US$ 430) and the maximum is Tanzania Shillings Five Billion (TZS 5,000,000,000, approx. US$ 2,150,000).[6]

1: Section 7(c) and (d) of the DPA
2: Section 45(1) and (2) of the DPA
3: Section 46 and 47 of the DPA
4: Section 50 of the DPA
5: Section 60(6)(a) and Section 61 of the DPA
6: Section 60(6)(b) of the DPA

ELECTRONIC MARKETING

The PDPA refers to regulations to be made relating to commercial use of personal data. It provides that a data subject can enter into a contract with a data controller for the processing of his / her personal data for pecuniary benefits or request a data controller to cease using his / her personal data for direct marketing in accordance with procedures to be set out in regulations to be made under the PDPA.[1]

The PDPA Regulations entitle a data subject to request a data controller or processor to erase or destroy the personal data held by them if the processing of such data is for commercial purposes and the data subject is unwilling for his data to be used commercially.[2] Where processing of personal data is by automated means for the purpose of evaluating matters related to a data subject or is likely to constitute the sole basis for any decision which significantly affects the subject, a data controller must also notify a data subject of the logic involved in that decision and their right to object to the use of their personal data in commercial advertisements.[3]

As advised above, the PDPA requires data controllers and processors to process personal data for the specific purpose for which it has been collected (*Please refer to our advice on Collection Processing of Data above on the requirements to be complied with by the data controllers and data processors while using personal data*). This implies that a person cannot use personal data obtained under the PDPA for commercial use, including electronic marketing, except with the consent from the data subject unless such use is authorised under any written law in Tanzania and the data subject has been informed of such use at the time the data was collected.

Further, financial services providers are prohibited from sharing consumers’ information with a third party for any purpose, including electronic marketing, unless such information is used for the purpose that is consistent with the purpose for which it was originally collected, and the prior written consent of the affected consumer has been obtained before such information is used for any promotional offers.[4]

1: Section 35 of the DPA
2: Regulation 17(d) of the PDPA Regulations
3: Section 33(1)(c) of the PDPA and regulation 19(2)(e) of the PDPA Regulations
4: Regulation 39(b) and (c), Financial Consumer Protection Regulations

ONLINE PRIVACY

Any use of cookies and other third-party trackers which can identify a natural person will qualify as disclosure of personal data and be subject to the PDPA. The PDPA requires data controllers and processors to process personal data for the specific purpose for which it has been collected (*Please refer to our advice on Collection Processing of Data above on the requirements to be complied with by the data collectors and data processors while using personal data*).

This implies that a person cannot use cookies and third-party trackers to process personal data except with the consent from the data subject unless such use is authorised under any written law in Tanzania and the data subject has been informed of such use at the time the data was collected. The data controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must also clearly describe the purpose for data processing for which consent is requested.

KEY CONTACTS

DLA Piper Africa, IMMMA Advocates
www.dlapiperafrica.co.tz/en/tanzania/

Madina Chenge
Partner
DLA Piper Africa, IMMMA Advocates
T +255 22 2211080/1/2/3
Madina.Chenge@immma.dlapiperafrica.co.tz

Miriam Bachuba
Senior Associate
DLA Piper Africa, IMMMA Advocates
T +255 22 2211080/1/2/3
Miriam.Bachuba@immma.dlapiperafrica.co.tz

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.