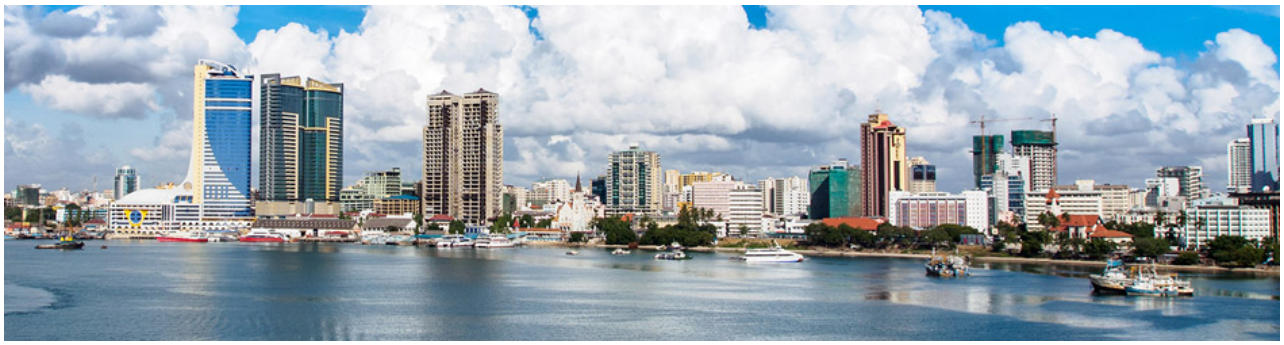
DATA PROTECTION LAWS OF THE WORLD

Tanzania

TANZANIA



Last modified 26 January 2023

LAW

On 27 November 2022, the Personal Data Protection Act was assented by the President of the United Republic of Tanzania into law ("**DPA**"). The DPA 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 Act, which include:

i. persona 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 DPA 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 collectors 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 Act is not yet operational as it will come into force on the date which the Minister responsible for communications will specify in the Government Gazette and such date has not been specified yet.

The DPA will be the national data protection law, 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 DPA defines "personal data" as any information relating to an identified or identifiable person that has been maintained in any manner, including such person's:

- personal information relating to race, national origin, ethnicity, religion, age or marital status;
- personal information relating to education, medical history, criminal or employment record;
- identification number, mark or other special method that identifies that person;
- address, fingerprints, or blood type;
- name appearing in the personal data of another person related to him or where disclosure of that name will disclose the personal data of that person; and
- information sent to a personal data collector that clearly shows such information is personal or confidential, and responses to that information would disclose the content of the previous information, and the views or opinions of any other person about the data subject.[1]

Definition of Sensitive Personal Data

The DPA defines "sensitive personal data" to include information:

- concerning genetics, children, offences, financial transactions of an individual or security steps, biometric information;
- which if processed, is personal information which shows a person's ethnic, social origin or race, political ideology, religious or philosophical beliefs, community, membership of workers' union, gender and health information or sexual relationships; and
- any personal information which according to the laws of the country is considered to have a significant impact on justice and interests of the individual to whom the information belongs.[2]

1: Section 3 of the DPA

2: Ibid

NATIONAL DATA PROTECTION AUTHORITY

The DPA provides for establishment of the Commission which will be responsible for monitoring and implementation of the provisions of DPA in Tanzania. The Commission is yet to be established. Hence, currently, the relevant authority still depends on the affected sector.

For instance, Tanzania Communications Regulatory Authority ("**TCRA**") is the national data protection authority in relation to electronic and postal communications and the Bank of Tanzania ("**BOT**") is the national data protection authority for financial services.

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 collectors or processors must appoint a data protection officer whose role is to ensure that control and security measures

are taken to protect personal information that is collected or processed.[1]

1: Section 27(3) of the DPA

COLLECTION & PROCESSING

The DPA requires the data collectors to collect personal data directly from the data subject.[1] The exception is where:

a. the personal data is already in the public domain;
b. the data subject has consented to the collection of his personal data from another person;
c. collection directly from the data subject has failed in the current circumstances;
d. the collection is authorised by law; and / or
e. collection directly from the data subject may affect the purpose for which the collection is sought.

Prior to collecting personal data, the collector must ensure that the data subject:

a. is aware and understands the purpose for which the personal data is being collected;
b. is aware the collection of personal data is for authorised purposes; and
c. knows the intended recipients of the personal data.[2]

Personal data collected can only be used for the intended purpose.[3] Where a collector collects personal data for any specified purpose, he can use such data for a different purpose provided:

i. the data subject has consented to the use of his personal data for such purpose;
ii. the use of the data for such purpose is authorised or required by law;
iii. there is a direct correlation between the purpose for which the personal data is used and that for which the data was collected;
iv. the information is used in a manner which does not identify the data subject;
v. the information is used for statistical or research purposes without identifying the data subject; and
vi. it is necessary to protect the vital interests (harm to health or life) of the data subject, another person or public health or security; or
vii. the use of such personal data is necessary for purposes of complying with the requirements of law.[4]

1: Section 23(1) of the DPA
2: Section 23(2) of the DPA
3: Section 25(1) of the DPA
4: Section 25(2) of the DPA

TRANSFER

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

a. to a country with an adequate personal data protection legal system (i.e. essentially equivalent levels of protection to that within Tanzania) provided the recipient has proven (i) such transfer is necessary for important reasons of public interest or any other legitimate purpose or (ii) 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 processing in the recipient country.[1] The data collector or processor must carry out a prior data protection impact assessment on the need to transfer 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]
b. to any other country with appropriate safeguards on the security and protection of personal data provided the data is

transferred to be processed for a purpose approved by the data subject,[4] unless the data subject has consented to such transfer, or the transfer is necessary:

i. for the performance of a contract between the data subject and the data collector or the implementation of pre-contractual measures taken at the request of the data subject;
ii. for the conclusion or performance of a contract concluded or to be concluded in the interest of the data subject between the collector and another person;
iii. for any public interest or the establishment, exercise or defence of a legal claim;
iv. to protect the vital interests of the data subject; or
v. in accordance with a law aimed at giving information to the public which affords an opportunity for public consultation in general or anyone with a legitimate interest to submit their comments in accordance with a procedure laid down by law.[5]

1: Section 31(2) of the DPA
2: Section 31(3) of the DPA
3: Section 31(5) of the DPA
4: Section 32(1) of the DPA
5: Section 32(4) of the DPA

SECURITY

The DPA requires data collectors 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. technological changes and the costs of implementing such measures; and
b. the type of personal data that should be protected and the harm that may occur to the data subject.[2]

Data collectors 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 collector in such a way that the data processor will carry out their activities under the instructions of the data collector and that the data processor will have a responsibility of ensuring compliance with the security standards provided under the DPA.[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 collectors must notify any personal data security breach to the Commission as soon as possible. The breaches notifiable are such security breaches which affect personal data being processed on behalf of the collector.[1]

Mandatory breach notification

As advised above, it is mandatory for every data collector to, as soon as possible, 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 DPA will have the authority to ensure implementation and enforcement of the provisions of the Act. The Commission has investigative and corrective powers including to:

a. receive, investigate and handle complaints related to contravention of personal data security and personal privacy; and
b. investigate and take necessary steps against anything it considers affects the security of personal data and privacy.[1]

The Commission is empowered to issue an enforcement notice on any person if satisfied that that such person has failed or is failing to comply with the provisions of the DPA. 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 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 collector 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 collector 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 collector or processor notified the Commissioner of the infringement;
h. the extent to which the data collector or processor had complied with previous enforcement or penalty notices;
i. adherence to approved codes of conduct or certification mechanisms;
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 avoided, 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 Million (TZS 1,000,000, approx. US$ 430).[3]

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

Violation of the DPA 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. £35) and the maximum is Tanzania Shillings Twenty Million (TZS 20,000,000, approx. £7,016). The maximum an individual may be sentenced for violating a provision under the DPA is ten (10) years. If found in violation of the DPA, an individual may be required to both pay a fine and serve a sentence.[5]

For a company or an organisation, the minimum fine for a violation is Tanzania Shillings One Million (TZS 1,000,000, approx. £351) and the maximum is Tanzania Shillings Five Billion (TZS 5,000,000,000, approx. £1,754,106).[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 DPA refers to regulations to be made relating to commercial use of personal data. It states a data subject can enter into a contract with a data collector for the processing of his personal data for commercial use or request a data collector to cease using his personal data for commercial use in accordance with procedures to be set out in regulations to be made under the DPA.[1] However, to date such regulations have not been issued.

As advised above, the DPA requires data collectors 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 personal data obtained under the DPA 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 obtains prior written consent of the consumer before using such information for future promotional offers.[2]

1: Section 35 of the DPA
2: Regulation 39(b) and (c), Financial Consumer Protection Regulations

ONLINE PRIVACY

Any use of cookies and other third party trackers in any which can identify a natural person will be subject to the DPA. The DPA requires data collectors 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 obtained under the DPA except with the consent from the data subject or 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.

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
chenge@immma.co.tz

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