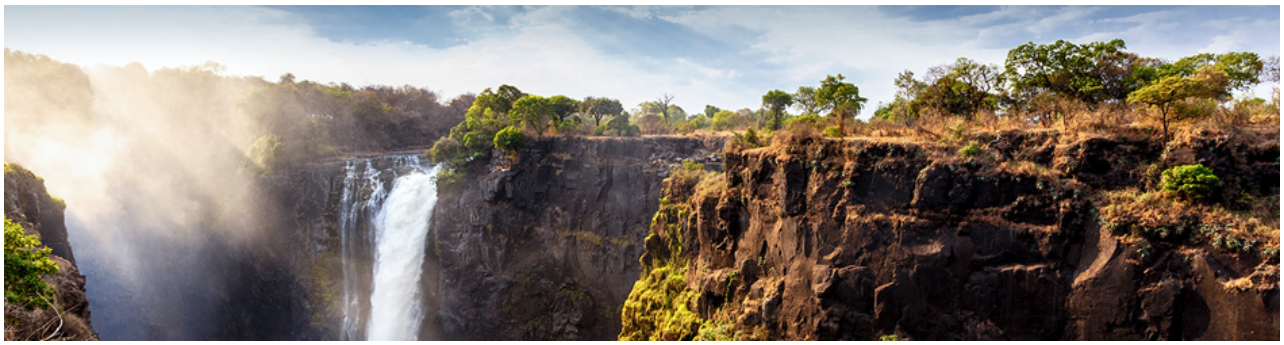
DATA PROTECTION LAWS OF THE WORLD

Zambia

ZAMBIA



Last modified 23 December 2021

LAW

Data Protection Act No. 3 of 2021 (the **“DPA"**).

DEFINITIONS

Definition of Personal Data

Data which relates to an individual who can be directly or indirectly identified from that data which includes a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of Sensitive Personal Data

Personal data which by its nature may be used to suppress the data subject’s fundamental rights and freedoms and includes:

- the race, marital status, ethnic origin or sex of a data subject;
- genetic data and biometric data;
- child abuse data;
- a data subject’s political opinions;
- a data subject’s religious beliefs or other beliefs of a similar nature;
- whether a data subject is a member of a trade union; or
- a data subject’s physical or mental health, or physical or mental condition.

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Data Protection Commissioner.

REGISTRATION

A person shall not control or process personal data without registering as a data controller or a data processor under the DPA.

DATA PROTECTION OFFICERS

Data controllers and data processors are required to appoint a data protection officer in line with the guidelines issued by the Data Protection Commissioner.

COLLECTION & PROCESSING

In order to collect or process personal data consent of the data subject must be obtained. A data subject may consent to such processing in writing. Prior to giving such consent, the data subject must be informed of the data subject’s right to withdraw the consent. Furthermore except as expressly provided in the DPA, a data controller is required to collect personal data directly from the data subject. The DPA provides additional rules in respect of collection and processing of personal data as set out below.

A data controller or data processor shall ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accurate and where necessary, kept up to date, with every reasonable step taken to ensure that any inaccurate personal data is erased or rectified without delay;
- stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;
- processed in accordance with the rights of a data subject; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against any loss, destruction or damage, using appropriate technical or organisational measures.

Subject to the other provisions of the DPA, a data controller may process personal data where:

- the data subject has given consent to the processing of that data subject’s personal data;
- the processing is necessary
    - for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
    - for compliance with a legal obligation to which the data controller is subject;
    - in order to protect the vital interests of the data subject or of another natural 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;
    - for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interest or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child; or
- the processing relates to personal data which is manifestly made public by the data subject.

A person shall not process sensitive personal data, unless:

- processing is necessary for the establishment, exercise or defence of a legal claim or whenever a court is exercising a judicial function;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; or
- processing is necessary for reasons of public interest.

Where a data subject is a child or a vulnerable person, that data subject’s right may be exercised by that data subject’s parents, legal guardian or a person exercising parental responsibility as the case may be. A data controller shall not process a child’s or vulnerable person’s personal data unless consent is given by the child’s or vulnerable person’s parent, legal guardian or a person exercising parental responsibility. A data controller shall, where the personal data of a child or a vulnerable person is involved, make every reasonable effort to verify that consent has been given or authorised, taking into account available technology. A data controller shall incorporate appropriate mechanisms for age verification and parental consent in the processing of personal data of a child.

TRANSFER

Transfer of personal data and sensitive personal data is subject to certain restrictions under the DPA. The DPA provides that personal data must be processed and stored on a server or data centre located in the Republic. The Minister may however prescribe categories of personal data that may be stored outside the Republic. The powers of the Minister notwithstanding, sensitive personal data must be processed and stored in a server or data centre located in the Republic.

Furthermore, the DPA provides that Personal data other than personal data categorised by the Minister may be transferred outside the Republic where:

- the data subject has consented and
    - the transfer is made subject to standard contracts or intragroup schemes that have been approved by the Data Protection Commissioner; or
    - the Minister, has prescribed that transfers outside the Republic is permissible; or
- the Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity.

Additional exceptions for the transfer of personal data outside the Republic are provided for, including:

- in case of an emergency, to a particular person or entity engaged in the provision of health services or emergency services;
- where the data subject has explicitly consented to that transfer of sensitive personal data; and
- to a particular international organisation or country which complies with the DPA, where the Data Protection Commissioner is satisfied that the transfer or class of transfers is necessary for any class of data controllers or data subjects and does not hamper the effective enforcement of the DPA.

SECURITY

A data controller or data processor is required to provide guarantees regarding the technical and organisational security measures employed to protect the personal data associated with the processing undertaken and ensure strict adherence to such measures.

A data controller or the data processor is further required to, having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement appropriate security safeguards including:

- maintaining integrity of personal data using methods including pseudonymisation and encryption;
- ensuring ongoing confidentiality, integrity and implementation of measures necessary to protect the integrity of personal data;
- measures necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data; and
- implementation of appropriate data protection policies.

A data controller and data processor is also required to undertake a periodic review of security safeguard in accordance with guidelines issued by the Data Protection Commissioner.

BREACH NOTIFICATION

A data controller shall notify the Data Protection Commissioner within twenty-four hours of any security breach affecting personal data processed.

A data processor shall notify the data controller, as soon as practicable of any security breach affecting personal data processed on behalf of the data controller.

A data controller or data processor shall notify the data subject, as soon as practicable of any security breach affecting personal data processed.

Mandatory breach notification

A data controller shall notify the Data Protection Commissioner within twenty-four hours of any security breach affecting personal data processed.

A data processor shall notify the data controller, as soon as practicable of any security breach affecting personal data processed on behalf of the data controller.

A data controller or data processor shall notify the data subject, as soon as practicable of any security breach affecting personal data processed.

ENFORCEMENT

The DPA sets out various penalties for offences prescribed thereunder. For example in respect of offences relating to the breach of the principles and rules relating to the processing of personal data, the penalty upon conviction is a fine not exceeding one hundred million penalty units[1] or two percent of annual turnover of the preceding financial year whichever is higher where the offence is committed by a corporate body.

Given that the DPA is a new piece of legislation, at the date of this update, we are not aware of any enforcement action taken by the Regulator.

---

[1] ZMW30,000,000 (at today’s exchange rate of US$1-ZMW16.37 approx. US$1,832,620.65)

ELECTRONIC MARKETING

Electronic marketing is governed by the Electronic Communications and Transactions Act No. 4 of 2021 (the “ ECTA’). The ECTA provides that a person marketing by means of electronic communication shall provide the addressee with:

- the person’s identity and contact details including its registered office and place of business, email, contact and customer service number;
- a valid and operational opt out facility from receiving similar communications in future;
- the identifying particulars of the source from which the originator obtained the addressee’s personal information; and
- applicable privacy and other user policies.

The ECTA also places restrictions in respect of unsolicited commercial communications to a consumer. The ECTA provides that a person may send one unsolicited commercial communication to a consumer, such commercial message can only be sent where the opt in requirement is met.

The ECTA further provides that an originator who sends unsolicited commercial communications to an addressee who has opted-out from receiving any further electronic communications from the originator through the originator’s opt out facility, commits an offence.

ONLINE PRIVACY

The ECTA provides that a service provider is not liable for any damage incurred by a person if the service provider refers or links users to a web page containing an infringing data message or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, and where the service provider:

- does not have actual knowledge that the data message or an activity relating to the data message is infringing the rights of that person;

- is not aware of facts or circumstances from which the infringing activity or the infringing nature of the data message is apparent;
- does not receive a financial benefit directly attributable to the infringing activity; and
- removes, or disables access to, the reference or link to the data message or activity within a reasonable time after being informed that the data message or the activity relating to that data message, infringes the rights of a person.

KEY CONTACTS

Chibesakunda & Co.
www.dlapiperafrica.com/zambia/

Louise De-Assis Chilepa
Head of Banking & Finance
T +260 211 366400
louise.chilepa@cco.co.zm

Mwamba Chibesakunda
Associate
T +260 211 366400
mwamba.chibesakunda@cco.co.zm

DATA PRIVACY TOOL

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