DATA PROTECTION LAWS OF THE WORLD

Zimbabwe

ZIMBABWE

Last modified 22 January 2024

LAW

Access to Information and Protection of Privacy Act (Chapter 10:27);

Banking Act (Chapter 24:20);

Courts and Adjudicating Authorities (Publicity Restrictions) Act (Chapter 07:04);

Consumer Protection Act (Chapter 14:44);

Census and Statistics Act (Chapter 10:29);

Cyber and Data Protection Act (Chapter 12:07);

Interception of Communications Act (Chapter 11:20); and,

National Registration Act (Chapter 10:17);

Communication Technology (“ICT Policy”).

DEFINITIONS

Definition of personal data

The Access to Information and Protection of Privacy Act defines personal information as recorded information about an identifiable person which includes:

- The person's name, address, or telephone number;
- The person's race, national or ethnic origin, religious or political beliefs or associations;
- The person's age, sex, sexual orientation, marital status, or family status;
- An identifying number, symbol or other particulars assigned to that person;
- Fingerprints, blood type or inheritable characteristics;
- Information about a person's healthcare history, including a physical or mental disability;
- Information about educational, financial, criminal or employment history;
- A third party's opinions about the individual;
- The individual's personal views or opinions (except if they are about someone else); and,
- Personal correspondence with home or family.

Definition of sensitive personal data

There is no law that defines Sensitive **Personal** Data. However, in terms of the Data Protection Act **sensitive data** refers to:

- information or any opinion about an individual which reveals or contains the following:
  - racial or ethnic origin;
  - political opinions;
  - membership of a political association;
  - religious beliefs or affiliations;
  - philosophical beliefs;
  - membership of a professional or trade association;
  - membership of a trade union;
  - sex life;
  - criminal educational, financial or employment history;
  - gender, age, marital status, or family status;
- health information about an individual;
- genetic information about an individual; or
- any information which may be considered as presenting a major risk to the rights of the data subject;

NATIONAL DATA PROTECTION AUTHORITY

In terms of the Data Protection Act, the Postal and Telecommunication Regulatory Authority established in terms of section 5 of the Postal and Telecommunications Act [Chapter 12:05]; is the recognised National Data Protection Authority. The Authority has the responsibility to promote and enforce the fair processing of personal data and advise the Minister of Information Communication Technology on matters relating to privacy rights. The Authority is mandated to conduct inquiries and investigations either on its own accord or on the request of any interested person in relation to data protection rights.

Under the recently enacted Draft Protection Act, a data protection officer must be appointed to ensure the compliance with all obligations provided for in the Data Protection Act.

The Zimbabwe Media Commission's mandate does the following:

- Ensures that the people of Zimbabwe have equitable and wide access to information;
- Comments on the implications of proposed legislation or programs of public bodies on access to information and protection of privacy; and,
- Comments on the implications of automated systems for collection, storage, analysis, or transfer of information or for the access to information or protection of privacy.

The Revised ICT Policy proposes the establishment of a quasi-government entity to monitor Internet traffic. It states that all Internet gateways and infrastructure will be controlled by a single company, while a National Data Centre to support both public and high security services and information will be established.

REGISTRATION

There is no law that requires the registration of databases.

DATA PROTECTION OFFICERS

In terms of the Data Protection Act, a Data Protection Officer refers to any individual appointed by the data controller and is charged with ensuring, in an independent manner, compliance with the obligations provided for in this Act.

COLLECTION & PROCESSING

There are no specific provisions for the collectors of personal data to obtain the prior approval of data subjects for the processing of their personal data. However, when collecting data the controller or the controller’s representative shall provide the data subject with at least the following information:

- the name and address of the controller and of his or her representative, if any;

- the purposes of the processing;
- the existence of the right to object, by request and free of charge, to the intended processing of data relating to him or her, if it is obtained for the purposes of direct marketing;
- whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;
- taking into account the specific circumstances in which the data is collected, any supporting information, as necessary to ensure fair processing for the data subject, such as:
    - the recipients or categories of recipients of the data;
    - whether it is compulsory to reply, and what the possible consequences of the failure to reply are;
    - the existence of the right to access and rectify the data relating to him or her except where such additional information, taking into account the specific circumstances in which the data is collected is not necessary to guarantee accurate processing.
- other information dependent on the specific nature of the processing, as specified by the Authority.

For purposes of processing the information Section 13 of the Data Protection Act is quite instructive. In terms of that Section every data controller or data processor shall ensure that personal information is:

- processed in accordance with the right to privacy of the data subject;
- processed lawfully, fairly and in a transparent manner in relation to any data subject;
- collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

The Census and Statistics Act contains provisions which restrict the use and disclosure of information obtained during the conducting of a census exercise. Under this Act, authorities are able to collect, compile, analyse, and abstract statistical information relating to any of the following:

- Commercial
- Industrial
- Agricultural
- Mining
- Social
- Economic
- General activities and conditions of the inhabitants of Zimbabwe and to publish such statistical information

TRANSFER

The transfer of data to any other jurisdiction is governed in terms of Part VII of the Data Protection Act under section 28 and 29.

In terms of Section 28 of the Data Protection Act:

- a data controller may not transfer personal information about a data subject to a third party who is in a foreign country unless an adequate level of protection is ensured in the country of the recipient or within the recipient international organisation and the
  data is transferred solely to allow tasks covered by the competence of the controller to be carried out.

- The adequacy of the level of protection afforded by the third country or international organisation in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; with particular consideration being given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country or recipient international organisation, the laws relating to data protection in force in the third country or international organisation in question and the professional rules and security measures which are complied with in that third country or international organisation.

- The Authority shall lay down the categories of processing operations for which and the circumstances in which the transfer of data to countries outside the Republic of Zimbabwe is not authorised.

- The Minister responsible for the Cyber security and Monitoring Centre in consultation with the Minister, may give directions on how to implement this section with respect to transfer of personal information outside of Zimbabwe.

SECURITY

Section 18 of the Data Protection Act provides guidelines for the protection of data. It states that to safeguard the security, integrity and confidentiality of the data, the controller or his or her representative, if any, or the processor, shall take the appropriate technical and organisational measures that are necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration, or access and any other unauthorised processing of the data.

Further the Section also provides that the Data Protection Authority may issue appropriate standards relating to information security for all or certain categories of processing. Since the enactment of this Act the Data Protection Authority is still to issue any appropriate standards.

The Revised ICT Policy states that there will be development, implementation and promotion of appropriate security and legal systems for e-commerce, including issues related to cybersecurity, data protection and e-transactions. The Policy states that the following laws will be enacted to cater for intellectual property rights, data protection and security, freedom of access to information, computer related and cybercrime laws:

- data protection and privacy
- intellectual property protection and copyright
- consumer protection and
- child online protection.

BREACH NOTIFICATION

Breach notification

Section 19 of the Data Protection Act places a duty on the data controller to notify the Authority “within twenty-four (24) hours of any security breach affecting data he or she processes.

Mandatory breach notification

Section 19 of the Data Protection Act uses the word “**shall**” which makes it mandatory to notify the Authority within twenty-four (24) hours.

ENFORCEMENT

The Constitution mandates the Human Rights Commission (HRC) to enforce a citizen's human rights where they have been violated. The right to privacy, including the right not to have the privacy of one's communication infringed, is a basic human right and, thus, falls within the purview of the HRC. However, the Cyber Security and Monitoring of Interceptions of Communications Centre (CSMICC), established by the Interception of Communications Act, is mandated to, among other things, monitor communications made over telecommunications, radio communications and postal systems and to give technical advice to service providers. The mandate of the CSMICC does not preclude it from monitoring computer-based data for the purposes of enforcing an individual's right to privacy where it is found that such right has been infringed.

Further, the CSMICC also has the duty to oversee the enforcement of the Act to ensure that it is enforced reasonably and with due regard to fundamental human rights and freedoms.

ELECTRONIC MARKETING

Zimbabwe recently enacted the Consumer Protection Act (Chapter 14:44) which has introduced several measures aimed at protecting consumers from unfair trade practices.

The Consumer Protection Act does not make specific reference to electronic marketing; however, it provides certain guidelines around electronic transactions, Information to be provided by the service provider, a cooling-off period in electronic transactions and unsolicited goods, services, or communications.

ONLINE PRIVACY

There is currently no specific online privacy legislation.

KEY CONTACTS

Manokore Attorneys
www.dlapiperafrica.com/en/zimbabwe/

Farai Nyabereka
Partner
Manokore Attorneys
T +263 4 746 787
fnyabereka@manokore.com

Steve Chikengezha
Associate
Manokore Attorneys
T +263 773 376 633
schikengezha@manokore.com

DATA PRIVACY TOOL

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