CHAPTER 12:07

CYBER AND DATA PROTECTION ACT

[Act re-gazetted with new title on 11 March 2022: Law reviser]

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

PART II

DATA PROTECTION AUTHORITY

PART III

QUALITY OF DATA

PART IV

GENERAL RULES ON THE PROCESSING OF DATA

PART V

DUTIES OF DATA CONTROLLER AND DATA PROCESSOR

PART VI

DATA SUBJECT

PART VII

TRANS BORDER FLOW

An Act to provide for data protection with due regard to the Declaration of Rights under the Constitution and the public and national interest; to establish a Cyber Security Centre; a Data Protection Authority and to provide for their functions; to create a technology driven business environment and encourage technological development and the lawful use of technology; to amend sections 162 to 166 of the Criminal Law (Codification and Reform) Act [*Chapter 9:23*] to provide for investigation and collection of evidence of cyber-crime and unauthorized data collection and breaches, and to provide for admissibility of electronic evidence for such offences; and to provide for matters connected with or incidental to the foregoing.

[Date of commencement: 3rd December, 2021]

PART I

PRELIMINARY

1 Short title

This Act may be cited as the Cyber and Data Protection Act [*Chapter 12:07*].

2 Object

The object of this Act is to increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects.

3 Interpretation

In this Act—

"child" means any person under the age of eighteen years;

"code of conduct" refers to the Data Use Charters drafted by the data controller in order to institute the rightful use of IT resources, the Internet, and electronic communications of the structure concerned, and which have been approved by the Data Protection Authority;

"consent" refers to any manifestation of specific unequivocal, freely given, informed expression of will by which the data subject or his or her legal, judicial or legally appointed representative accepts that his or her data be processed;

"critical database" means a computer data storage medium or any part thereof which contains critical data;

"data" means any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data;

"data controller" or "controller"—

(*a*) refers to any natural person or legal person who is licensable by the Authority;

(*b*) includes public bodies and any other person who determines the purpose and means of processing data;

"data controller's representative" or "controller's representative" refers to any natural person or legal person who performs the functions of the data controller in compliance with obligations set forth in this Act;

"Data processor" refers to a natural person or legal person, who processes data for and on behalf of the controller and under the controller's instruction, except for the persons who, under the direct employment or similar authority of the controller, are authorised to process the data;

"Data Protection Authority" or "Authority" refers to Postal and Telecommunications Regulatory Authority of Zimbabwe established in terms of section 5 of the Postal and Telecommunications Act [*Chapter 12:05*];

"data protection officer" or "DPO" 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;

"data subject" refers to an individual who is an identifiable person and the subject of data;

"disproportionate effort" means effort that is so labour intensive as to consume a lot of time, money and manpower resources;

"electronic communications network" means any electronic communication infrastructure and facilities used for the conveyance of data;

"genetic data: refers to any personal information stemming from a Deoxyribonucleic acid (DNA) analysis;

"health professional" refers to any individual determined as such in terms of the Health Professions Act [*Chapter 27:19*];

"identifiable person" means a person who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity;

"Minister" means the Minister responsible for information and communications technologies;

"personal information" means information relating to a data subject, and includes—

(*a*) the person's name, address or telephone number;
(*b*) the person's race, national or ethnic origin, colour, religious or political beliefs or associations;
(*c*) the person's age, sex, sexual orientation, marital status or family status;
(*d*) an identifying number, symbol or other particulars assigned to that person;
(*e*) fingerprints, blood type or inheritable characteristics;
(*f*) information about a person's health care history, including a physical or mental disability;
(*g*) information about educational, financial, criminal or employment history;
(*h*) opinions expressed about an identifiable person;
(*i*) the individual's personal views or opinions, except if they are about someone else; and
(*j*) personal correspondence pertaining to home and family life;

"processing" refers to any operation or set of operations which are performed upon data, whether or not by automatic means, such as obtaining recording or holding the data or carrying out any operation or set of operations on data, including—

(*a*) organisation, adaptation or alteration of the data;
(*b*) retrieval, consultation or use of the data; or
(*c*) alignment, combination, blocking, erasure or destruction of the data;

"recipient" a natural or legal person, agency or any other body to whom personal information is disclosed by a data controller, whether a third party or not; however, persons who receive personal information in the framework of a particular legal inquiry shall not be regarded as recipients;

"sensitive data" refers to—

(*a*) information or any opinion about an individual which reveals or contains the following—
  (i) racial or ethnic origin;
  (ii) political opinions;
  (iii) membership of a political association;
  (vi) religious beliefs or affiliations;
  (v) philosophical beliefs;
  (vi) membership of a professional or trade association;
  (vii) membership of a trade union;
  (viii) sex life;
  (ix) criminal educational, financial or employment history;
  (x) gender, age, marital status or family status;
(*b*) health information about an individual;

(*c*) genetic information about an individual; or

(*d*) any information which may be considered as presenting a major risk to the rights of the data subject;

"third party" refers to any natural or legal person or organisation other than the data subject, the controller, the processor and anyone who, under the direct authority of the controller or the processor, is authorised to process the data;

"trans-border flow" refers to international flows of data by the means of transmission including data transmission electronically or by satellite;

"whistleblowing" refers to legal provisions permitting individuals to report the behaviour of a member of their organisation which, they consider contrary to a law or regulation or fundamental rules established by their organisation.

4 Application

(1) This Act shall apply to matters relating to access to information, protection of privacy of information and processing and storage of data wholly or partly by automated means: and shall be interpreted as being in addition to and not in conflict or inconsistent with the Freedom of Information Act [*Chapter 10:33*].

(2) Subject to subsection (1) this Act shall be applicable—

(*a*) to the processing of data carried out in the context of the effective and actual activities of any data controller;

(*b*) to the processing and storage of data by a controller who is not permanently established in Zimbabwe, if the means used, whether electronic or otherwise is located in Zimbabwe, and such processing and storage is not for the purposes of the mere transit of data through Zimbabwe.

(3) In the circumstances referred to in subsection (2)(b), the controller shall designate a representative established in Zimbabwe, without prejudice to legal proceedings that may be brought against the controller.

PART II

DATA PROTECTION AUTHORITY

5 Designation of Postal and Telecommunications Regulatory Authority as Data Protection Authority

The Postal and Telecommunications Regulatory Authority established in terms of the Postal and Telecommunications Act [*Chapter 12:05*] is hereby designated as the Data Protection Authority.

6 Functions of Data Protection Authority

(1) The Authority shall perform the following functions—

(*a*) to regulate the manner in which personal information may be processed through the establishment of conditions for the lawful processing of data;

(*b*) to promote and enforce fair processing of data in accordance with this Act;

(*c*) to issue its opinion either of its own accord, or at the request of any person with a legitimate interest, on any matter relating to the application of the fundamental principles of the protection of privacy, in the context of this Act;

(*d*) to submit to any Court any administrative act which is not compliant with the fundamental principles of the protection of the privacy in the frame- work of this Act as well as any law containing provisions regarding the protection of privacy in relation to the processing of data in consultation with Minister responsible for Information, Publicity and Broadcasting Services;

(*e*) to advise the Minister on matters relating to right to privacy and access to information;

(*f*) to conduct inquiries or investigations either of its own accord or at the request of the data subject or any interested person, and in relation thereto may call upon the assistance of experts to carry out its functions and may request the disclosure of any documents that may be of use for their inquiry or investigation;

(*g*) to receive, by post or electronic means or any other equivalent means, the complaints lodged against data processing and give feed-back to the claimants or complainants;

(*h*) to investigate any complaint received in terms of this Act howsoever received;

(*i*) to conduct research on policy and legal matters relating to the development of international best practices on the protection of personal information in Zimbabwe and advise the Minister accordingly;

(*j*) in consultation with the Minister, to facilitate cross border cooperation in the enforcement of privacy laws and participating at national, regional and international forums mandated to deal with the protection of personal information initiatives.

(2) Subject to this Act, the Authority shall not, in the lawful exercise of its functions under this Act, be subject to the direction or control of any person or authority.

PART III

QUALITY OF DATA

7 Quality of Data

(1) The data controller shall ensure that data processed is—

(*a*) adequate, relevant and not excessive in relation to the purposes for which it is collected or further processed;

(*b*) accurate and, where necessary, kept up-to-date;

(*c*) retained in a form that allows for the identification of data subjects, for no longer than necessary with a view to the purposes for which the data is collected or further processed.

(2) The data controller shall take all appropriate measures to ensure that data processed shall be accessible regardless of the technology used and ensure that the evolution of technology shall not be an obstacle to the access or processing of such data.

(3) The controller shall ensure compliance with the obligations set out in subsections (1) and (2) by any person working under his or her authority and any subcontractor.

PART IV

GENERAL RULES ON THE PROCESSING OF DATA

8 Generality

The data controller shall ensure that the processing of data is necessary and that the data is processed fairly and lawfully.

9 Purpose

(1) The data controller shall ensure that data is collected for specified, explicit and legitimate purposes and, taking into account all relevant factors, especially the reasonable expectations of the data subject and the applicable legal and regulatory provisions, that the data is not further processed in a way incompatible with such purposes.

(2) Under the conditions established by the Authority, further processing of data for historical, statistical or scientific research purposes is not considered incompatible.

10 Non-sensitive data

(1) Personal information may only be processed if the data subject or a competent person, where the data subject is a child, consents to the processing of such data.

(2) The consent referred to in subsection (1) may be implied where the data subject is an adult natural person or has a legal persona and has full legal capacity to consent.

(3) The processing of non-sensitive data is permitted, without the consent of the data subject, where necessary for purposes of—

(*a*) being material as evidence in proving an offence; or

(*b*) compliance with an obligation to which the controller is subject by or by virtue of a law; or

(*c*) protecting the vital interests of the data subject; or

(*d*) performing a task carried out in the public interest, or in the exercise of the official authority vested in the controller, or in a third party to whom the data is disclosed; or

(*e*) promoting the legitimate interests of the controller or a third party to whom the data is disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject claiming protection under this Act.

(4) The Authority may specify the circumstances in which the condition stipulated under subsection (3)(e) are considered as having been met.

11 Sensitive information

(1) No data controller shall process sensitive data unless the data subject has given consent in writing for such processing;

(2) The consent to the processing of data may be withdrawn by the data subject at any time and without any explanation and free of charge;

(3) The Authority shall determine the circumstances in which the prohibition to process the data referred to in this subsection (1) cannot be lifted even with the data subject's consent (taking into account the factors surrounding the prohibition and the reasons for collecting the data).

(4) 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 sensitive information affecting national security or the interests of the State.

(5) The provisions of subsection (1) shall not apply where—

(*a*) the processing is necessary to carry out the obligations and specific rights of the controller in the field of employment law; or

(*b*) the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving his or her consent or is not represented by his or her legal, judicial or agreed representative; or

(*c*) the processing is carried out in the course of its legitimate activities by a foundation, association or any other non-profit organisation with a political, philosophical, religious, health-insurance or trade-union purpose and on condition that the processing relates solely to the members of the organisation or to persons who have regular contact with it in connection with such purposes and that the data is not disclosed to a third party without the data subjects' consent; or

(*d*) the processing is necessary to comply with national security laws; or

(*e*) the processing is necessary, with appropriate guarantees, for the establishment, exercise or defence of legal claims; or

(*f*) the processing relates to data which has been made public by the data subject; or

(*g*) the processing is necessary for the purposes of scientific research:

Provided the Authority shall be entitled to specify the conditions under which such processing may be carried out; or

(*h*) the processing of data is authorised by a law or any regulation for any other reason constituting substantial public interest.

(6) Without prejudice to the application of sections 5 to 8, the processing of data relating to sex life is authorised if—

(*a*) it is carried out by an association with a legal personality or by an organisation of public interest whose main objective, according to its Memorandum and Articles of Association, is the evaluation, guidance or treatment of persons of such sexual conduct, and who is recognised by a competent public body as being responsible for the welfare of such persons;

(*b*) the objective of the processing of the data consist of the evaluation, guidance and treatment of the persons referred to in this section, and the processing of data relates only to the afore-mentioned persons:

Provided that the competent public body referred to in paragraph (a) grants a specific, individualised authorisation, having received the opinion of the Authority.

(7) The authorisation referred to in this section shall specify the duration of the authorisation, the conditions for supervision of the authorised association or organisation by the competent public body, and the way in which the processing must be reported to the Authority.

12 Genetic data, biometric sensitive data and health data

(1) The processing of genetic data, biometric data and health data is prohibited unless, the data subject has given consent in writing to the processing.

(2) The consent referred to in subsection (1) can be withdrawn by the data subject at any time without any reasons and free of charge.

(3) The provisions of subsection (1) shall not apply where—

(*a*) the processing is necessary to carry out the specific obligations and rights of the controller in the field of employment law; or

(*b*) the processing is necessary to comply with national security laws; or

(c) the processing is necessary for the promotion and protection of public health, including medical examination of the population; or

(*d*) the processing is required by or by virtue of a law or any equivalent legislative act for reasons of substantial public interest; or

(*e*) the processing is necessary to protect the vital interests of the data subject or another person, where the data subject is physically or legally incapable of giving his or her consent or is not represented by his or her legal, judicial or agreed representative; or

(*f*) the processing is necessary for the prevention of imminent danger or the mitigation of a specific criminal offence; or

(g) the processing relates to data which has apparently been made public by the data subject; or

(*h*) the processing is necessary for the establishment, exercise or defense of legal rights; or

(*i*) the processing is required for the purposes of scientific research; or

(*j*) the processing is necessary for the purposes of preventive medicine or medical diagnosis, the provision of care or treatment for the data subject or to one of his or her relatives, or the management of health-care services in the interest of the data subject, and the data is processed under the supervision of a health professional.

(4) Health-related data may only be processed under the responsibility of a health-care professional, except if the data subject has given his or her written consent or if the processing is necessary for the prevention of imminent danger or for the mitigation of a specific criminal offence.

(5) The Authority shall be entitled to specify the conditions under which such processing may be carried out.

(6) Health related data may only be collected from other sources where the data subject is incapable of providing the data.

(7) For the purposes of processing personal information under this section, the health professional and his or her agents are subject to the duty of professional secrecy.

(8) The processing of genetic data, shall be authorised if it is processed for what it reveals or contains and data concerning health shall be processed only if a unique patient identifier is given to the patient which is distinct from any other identification number, issued by the public authority established for this purpose.

(9) The association of the unique patient identifier with any other identifier which permits the identification of the data subject as provided for in section 8 is permissible only with the express authorisation of the Authority.

(10) The data of a child shall be processed subject to section 26.

PART V

DUTIES OF DATA CONTROLLER AND DATA PROCESSOR

13 Duties of Data Controller

Every data controller or data processor shall ensure that personal information is—

(*a*) processed in accordance with the right to privacy of the data subject;

(*b*) processed lawfully, fairly and in a transparent manner in relation to any data subject;

(*c*) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;

(*d*) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;

(*e*) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;

(*f*) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; and

kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected.

14 Rights of Data Subject

A data subject has a right to—

(*a*) be informed of the use to which their personal information is to be put;

(*b*) access their personal information in custody of data controller or data processor;

(*c*) object to the processing of all or part of their personal information;

(*d*) correction of false or misleading personal information; and;

(*e*) deletion of false or misleading data about them.

15 Disclosures when collecting data directly from data subject

(1) When obtaining data directly from the data subject, the controller or the controller's representative shall provide the data subject with at least the following information, unless the data subject has already received such information—

(*a*) the name and address of the controller and of his or her representative, if any;

(*b*) the purposes of the processing;

(*c*) 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;

(*d*) whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;

(*e*) 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—

(i) the recipients or categories of recipients of the data;

(ii) 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.

(*f*) other information dependent on the specific nature of the processing, as specified by the Authority.

16 Disclosures when not collecting data directly from data subject

(1) Where the data is not collected from the data subject, the controller or his or her representative shall provide the data subject with at least the information set out below when recording the data or considering communication to a third party, unless it is established that the data subject is in receipt of such information—

(*a*) the name and address of the controller and of his or her representative, if any;

(*b*) the purposes of the processing;

(*c*) whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;

(*d*) 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; in which case, the data subject shall be informed prior to the first disclosure of the data to a third party or prior to the first use of the data for the purposes of direct marketing on behalf of third parties;

(*e*) taking into account the specific circumstances in which the data is collected, any supporting information, as necessary to ensure fair processing such as—

(i) the categories of data concerned;

(ii) the recipients or categories of recipients of the data;

(iii) the existence of the right to access and rectify the data relating to him/her, unless such additional information, taking into account the specific circumstances in which the data is provided, is not necessary to guarantee fair processing with respect to the data subject;

(*f*) other information dependent on the specific nature of the processing, which is specified by the Authority.

(2) The provisions of subsection (1) shall not apply where—

(*a*) informing the data subject proves impossible or would involve a disproportionate effort, in particular for data collected for statistical purposes or for the purpose of historical or scientific research, or for the purpose of medical examination of the population with a view to protecting and promoting public health; or

(*b*) data is recorded or provided in terms of the law;

(3) The Authority shall establish the conditions for the application of this section.

17 Authority to process

Any person having access to the data and acting under the authority of the controller or of the processor, as well as the processor himself or herself, may process data only as instructed by the controller, without prejudice to any duty imposed by law.

18 Security

(1) In order 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.

(2) These measures referred to in subsection (1) must ensure an appropriate level of security taking into account the state of technological development and the cost of implementing the measures on the one hand, and the nature of the data to be protected and the potential risks to the data subject on the other hand.

(3) The Authority may issue appropriate standards relating to information security for all or certain categories of processing.

(4) The data controller shall appoint data processor who provide sufficient guarantees regarding the technical and organisational security measures employed to protect the data associated with the processing undertaken and ensure strict adherence to such measures.

(5) The data controller shall enter into a written contract or any other legal instrument with the data processor which ensures that the data processor maintains security measures on data.

19 Security breach notification

The data controller shall notify the Authority "within twenty-four (24) hours of any security breach affecting data he or she processes.

20 Obligation of notification to Authority

(1) Prior to any wholly or partly automated operation or set of operations intended to serve a single purpose or several related purposes, the controller or his or her representative, if any, must notify the Authority.

(2) Any modification to the information provided according to section 16 must be notified to the Authority.

(3) The provisions of subsection (1) shall not apply to operations having the sole purpose of keeping a register that is intended to provide information to the public by virtue of operation of law and that is open to access by the general public or by any person demonstrating a legitimate interest.

(4) The Authority may exempt certain categories from notification under this section if—

(*a*) taking into account the data being processed, there is no apparent risk of infringement of the data subjects' rights and freedoms, and if the purposes of the processing, the categories of data being processed, the categories of data subjects, the categories of recipients and the data retention period are specified;

(*b*) the data controller has appointed a data protection officer.

(5) The appointment of the data protection officer shall be duly notified to the Authority.

The Authority shall provide guidelines that provide for the qualifications and functions of data protection officer and such data protection officer's duties shall include—

a ensuring compliance by the data controller with the provisions of this Act and regulations made thereunder;

b dealing with requests made to the data controller pursuant to this Act;

c working with the Authority in relation to the performance of its functions in relation to the data controller.

(6) If exemption from the duty of notification has been granted for automatic processing in accordance with the subsection 3, the data controller may disclose the items of information mentioned in section 16 to any person entitled to receive such information.

22 Content of notification

(1) The notification referred to in section 20 shall state, at least—

(*a*) the date of notification and the law or regulatory instrument permitting the automatic processing of data;

(*b*) the surname, first names and complete address or the name and registered offices of the controller and of his or her representative, if any;

(*c*) the denomination of the automatic processing;

(*d*) the purpose or the set of related purposes of the automatic processing;

(*e*) the categories of data being processed and a detailed description of the sensitive data being processed;

(*f*) a description of the category or categories of the data subjects;

(*g*) the safeguards that must be linked to the disclosure of the data to third parties;

(*h*) the manner in which the data subjects are informed, the service providing for the exercise of the right to access and the measures taken to facilitate the exercise of that right;

(*i*) the inter-related processing planned or any other form of linking with other processing;

(j) the period of time after the expiration of which the data may no longer be stored, used or disclosed;

(*k*) a general description containing a preliminary assessment of whether the security measures provided for pursuant to section 13 above are adequate;

(*l*) the recourse to a data processor, if any;

(*m* the transfers of data to a third country as planned by the data controller.

(2) The Authority may prescribe other information which shall be mentioned in the notification.

(3) Where the Authority is of the opinion that the processing or transfer of data by a data controller entails specific risks to the privacy rights of data subjects, he or she may inspect and assess the security and organisational measures prior to the commencement of the processing or transfer.

(4) The Authority may, during working hours, carry out further inspection and assessment of the security and organisational measures employed by a data controller subject to reasonable notification to the data controller of the Authority's intended inspection and assessment.

22 Authorisation

(1) The Authority shall establish the categories of data processing which represent specific risks to the fundamental rights of the data subject and which require specific authorisation from the Authority.

(2) Such authorisation shall only be provided following receipt of notification from the data controller or from the data protection officer pursuant to sections 15 and 16.

23 Openness of processing

(1) The Authority shall keep a register of all automatic processing operations of data.

(2) Any entry in the register referred to in subsection (1) must include the information mentioned in section 16(1).

(3) The register shall be available for inspection by members of the public, in the manner determined by the Authority.

(4) In case of the processing of data exempted from notification by this Act, the Authority may, either by virtue of its office or at the data subject's request, impose upon the controller the obligation to disclose to the data subject all or part of the information mentioned in section 16(1).

24 Accountability

(1) The data controller shall—

(*a*) take all the necessary measures to comply with the principles and obligations set out in this Act; and

(*b*) have the necessary internal mechanisms in place for demonstrating such compliance to both the data subjects and the Authority in the exercise of its powers.

PART VI

DATA SUBJECT

25 Decision taken on basis of Automatic Data Processing

(1) The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

(2) The right referred to in subsection (1) shall not be applicable if the decision based solely on automated processing is taken on the basis of the data subject having consented to such decision or is based on a provision established by law.

26 Representation of data subject who is child

Where the data subject is a child, his or her rights pursuant to this law may be exercised by his or her parents or legal guardian.

27 Representation of physically, mentally or legally incapacitated data subjects

(1) A data subject who is physically, mentally or legally incapable of exercising the rights given under this Act and who is not subject to the provisions of section 26, may exercise such rights through a parent or guardian or as provided for by law or as designated by a Court of competent jurisdiction.

(2) Incapacity as referred to in subsection (1) shall be proven by a physician or a person legally competent to do so.

TRANS-BORDER FLOW

28 Transfer of personal information outside Zimbabwe

(1) Subject to the provisions of this 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.

(2) 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.

(3) 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.

(4) 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.

29 Transfer to country outside Zimbabwe which does not assure adequate level of protection

(1) A transfer or a set of transfers of data to a country outside Zimbabwe which does not assure an adequate level of protection may take place in one of the following cases—

(*a*) the data subject has unambiguously given his or her consent to the proposed transfer;

(*b*) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken in response to the data subject's request;

(*c*) the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the controller and a third party in the interest of the data subject;

(*d*) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims;

(*e*) the transfer is necessary in order to protect the vital interests of the data subject;

(*f*) the transfer is made from a register which, according to acts or regulations, is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the case at hand.

PART VIII

CODE OF CONDUCT

30 Code of Conduct

(1) The Authority shall provide guidelines and approve codes of conduct and ethics governing the rules of conduct to be observed by data controllers and categories of data controllers.

(2) In effecting (1) above, the Authority shall consider trade associations and other bodies representing other categories of controllers who have national codes or have the intention of amending or extending existing national codes and allow them to submit such codes for the approval of the Authority.

(3) The Authority in considering codes of conduct for approval, shall ascertain, among other things, whether the Codes submitted comply with the provisions of this Act.

(4) If it deems it fit, the Authority shall seek the views of affected data subjects or their representatives.

PART IX

WHISTLEBLOWING

31 Whistle-blower

(1) The Authority shall establish rules giving the authorisation for and governing the whistleblowing system.

(2) Rules established in terms of subsection (1) must preserve—

(*a*) the principles of fairness, lawfulness and purpose of the processing;

(*b*) the principles related to the proportionality on the limitation of the scope, accuracy of the data which will be processed;

(*c*) the principle of openness and delivering an adequate system for the collection of personal information shall address—

(i) the scope and purpose of the whistleblowing;

(ii) the processing of reporting;

(iii) the consequences of the justified and unjustified reporting;

(iv) the way of exercising the rights of access, correction, deletion as well as the competent authority to which a request can be made; and

(v) the third party who may receive data concerning the informer and the person who is implicated in the scope of the processing of the report;

(vi) the technical and organisational rules;

(vii) rules concerning the rights of the data subject by making clear that the right of access doesn't allow to access to data linked to a third person without his or her express and written consent; and

(viii) the method of notifying the Authority.

(3) The person who is implicated shall be informed as soon as possible of the existence of the report and about the facts which he or she is accused of in order to exercise the rights established in this Act.

(4) The release of information to the person who is implicated may be withheld in exceptional circumstances.

PART X

GENERAL PROVISIONS

32 Regulations

(1) The Minister may, in consultation with the Authority, make regulations providing for all matters which by this Act are required or permitted to be prescribed or which, in his or her opinion, are necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) Regulations referred to in subsection (1) may provide for the exercise of the rights referred to in sections 25 to 27 of the Act.

33 Offences and penalties

(1) Any member of staff of the Authority or any expert, contractor, sub- contractor who violates the provisions of this Act shall be guilty of an offence and liable to a fine not exceeding level 7 or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(2) Any data controller, his or her representative, agent or assignee who contravenes section 11, 13, 18(4), 24 and 28 shall be guilty of an offence and liable to a fine not exceeding level 11 or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.

(3) Upon conviction by a Court of competent jurisdiction the Court may order the seizure of the media containing the data to which the offence relates, such as manual filing systems, magnetic discs or magnetic tapes, except for computers or any other equipment, or the deletion of the data.

(4) Seizure or deletion may be ordered where the media containing the data does not belong to the person convicted.

(5) The objects seized in terms of this section shall be destroyed.

(6) The controller or his or her representative shall be liable for the payment of the fines incurred by his or her agent or assignee.

34 Appeals

Any person aggrieved by the decision of the Authority may appeal to the Administrative Court.