CHAPTER [INSERT]
DATA PROTECTION BILL
Acts [insert]

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

1.	Short Title
2.	Interpretation
3.	Scope of Application

PART II

DATA PROTECTION AUTHORITY

4.	Establishment of Data Protection Authority of Zimbabwe
5.	Functions of the Authority
6.	Establishment of Data Protection Authority of Zimbabwe Board
7.	Constitution of Board
8.	Terms of office and conditions of service of members
9.	Disqualifications for appointment as member
10.	Vacation of office by member
11.	Dismissal or suspension of members
12.	Access to the Authority
13.	Penalties
14.	Financial Provisions

PART III

QUALITY OF THE DATA

15.	Quality of the Data

PART IV
GENERAL RULES ON THE PROCESSING OF PERSONAL DATA

16.	Generality
17.	Purpose
18.	Non-sensitive data
19.	Sensitive information
20.	Genetic data, biometric sensitive data and health data

PART V
DUTIES OF THE DATA CONTROLLER AND DATA PROCESSOR

21.	Disclosures when collecting data directly from the data subject
22.	Disclosures when not collecting data directly from the data subject
23.	Authority to process
24.	Security
25.	Security breach notification
26.	Obligation of notification to the Authority
27.	Content of the notification
28.	Authorization
29.	Openness of the processing
30.	Accountability

PART VI
RIGHTS OF THE DATA SUBJECT

31.	Right of access
32.	Right of rectification, deletion and temporary limitation of access
33.	Right of objection
34.	Delays
35.	Further Regulation
36.	Decision taken purely on the basis of automatic data processing
37.	Representation of the data subject who is a child
38.	Representation of physically, mentally or legally incapacitated data subjects

PART VII
RECOURSE TO THE JUDICIAL AUTHORITY

39.	Recourse to the judicial authority

PART VIII
SANCTIONS

40.	Penalties

PART IX
LIMITATIONS

41.	Limitations

PART X
TRANSBORDER FLOW

42.	To a Member State which has transposed the SADC Model Law
43.	To a Member state which has not transposed the SADC Model Law or to a non SADC Member State
44.	Transfer to a country outside the SADC which does not assure an adequate level of protection

PART XI
CODE OF CONDUCT

45.	Code of Conduct

PART XII
WHISTLEBLOWING

46.	Whistleblowing

AN ACT to govern the processing of personal information by private and public bodies, to prevent unauthorised and arbitrary use, collection, processing, transmission and storage of data of identifiable persons, to provide for the regulation of data protection, to establish a Data Protection Authority and to provide for matters connected therewith or incidental to the foregoing.

PART I

PRELIMINARY

1	**Short Title**	This legislation may be cited as the Data Protection Act, and shall come into force and effect [on xxx/ following publication in the *Gazette*].
2	**Interpretation**	(1) **Child:** refers to a person under the age of sixteen years and includes an infant (2**) 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. (3) **Consent:** refers to any manifestation of specific, unequivocal, freely given, informed expression of will by which the data subject or his/her legal, judicial or legally appointed representative accepts that his/her personal data be processed. (4) **Data:** refers to all representations of information notwithstanding format or medium. (5) **Data controller or controller:** refers to any natural person and legal person excluding a public body which alone or jointly with others determines the purpose and means of processing of personal data. Where the purpose and means of processing are determined by or by virtue of an act, decree or ordinance, the controller is the natural person, legal person or public body designated as such by virtue of that act, decree or ordinance. (6) **Data controller's representative or controller's representative:** refers to any natural person or legal person permanently established on the territory of Zimbabwe, who performs the functions of the data controller in compliance with obligation(s) set forth in this Act. (7) **Data processor:** refers to a natural person or legal person, which processes personal data for and on behalf of the controller and under the data controller's instruction, except for the persons who, under the direct employment or similar authority of the controller, are authorised to process the data. (8) **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 law. (9) **Data subject:** refers to an individual who is an identifiable person and the subject of personal data. (10) **Identifiable person:** (a) is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity. (b) To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the said person. (11) **Genetic data:** refers to any personal information stemming from a Deoxyribonucleic acid (DNA) analysis. (12) **Health professional:** refers to any individual determined as such by Zimbabwean law.

(13) **Personal information:** 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.
(14) **Processing:** refers to any operation or set of operations which is performed upon personal 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) organization, 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.
(15) **Protection Authority or Authority:** refers to an independent authority established by Part II of this Act.
(16) **Recipient:** is 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 which receive personal information in the framework of a particular legal inquiry shall not be regarded as recipients.
(18) **Register:** means the register referred to in Part III of this Act.
(19) **Sensitive data:**
refers to (a) information or an opinion about an individual which reveals or contains the following
(i) racial or ethnic origin;
(ii) political opinions;
(iii) membership of a political association;
(iv) 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
; or
(b) health information about an individual;
(c) genetic information about an individual; or
(d) information which may be considered as presenting a major risk to the rights of the data subject.

(20) **Third party:** refers to any natural or legal person or organization other than the data subject, the controller, the processor and anyone who, under the direct authority of the controller or the processor, is authorized to process the data.
(21) **Transborder flow:** refers to international flows of personal data by the means of transmission including data transmission electronically or by satellite.
(22) **Whistleblowing:** refers to legal provisions permitting individuals to report the behaviour of a member of their organization which, they consider contrary to a law or regulation or fundamental rules established by their organization.

3 Scope of Application

(1) This Act shall apply to matters relating to access to information, protection of privacy of information and processing of personal data wholly or partly by automated means; and shall be interpreted as being in addition to and not in substitution for any other law which is not in conflict or inconsistent with this Act.
(2) This Act is applicable:
(a) to the processing of personal data carried out in the context of the effective and actual activities of any controller permanently established in Zimbabwe or in a place where Zimbabwean law applies by virtue of international public law;
(b) to the processing of personal 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 is not for the purposes of mere transit of personal data through Zimbabwe.
(3) In the circumstances referred to in the previous paragraph under (2)b, the controller shall designate a representative established in Zimbabwe, without prejudice to legal proceedings that may be brought against the controller.

(4) This Act cannot restrict:
(a)the ways of production of information which are available according to a national law or as permitted in the rules that govern legal proceedings; and
(b) the power of the judiciary to constrain a witness to testify produce evidence.

PART II:

DATA PROTECTION AUTHORITY

4	**Establishment of Data Protection Authority of Zimbabwe**	(1) There is hereby established an independent authority, to be known as the Data Protection Authority of Zimbabwe which shall be a body corporate capable of suing and being sued in its corporate name and, subject to this Act, of performing all acts that bodies corporate may by law perform.
5	**Functions of the Authority**	(1) Subject to this Act, the functions of the Authority shall be- (a) to promote and enforce fair processing of personal data in accordance with this Act; (b) 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; (c) to submit to the Court any administrative act which is not compliant with the fundamental principles of the protection of the privacy in the framework of this Act as well as any law containing provisions regarding the protection of privacy in relation to the processing of personal data in consultation with Minister responsible for Access to Information and Protection of Privacy Act Chapter 10:27; (d) to advise the Minister on matters relating to right to privacy and access to information; (e) to conduct inquiries/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/ investigation. (f) to receive, by post or electronic means or any another equivalent means, the complaints lodged against a personal data processing and give feed-back to the claimants/complainants. (g) to investigate any complaint received in terms of this Act howsoever received; (h)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.
6	**Establishment of Data Protection Authority of Zimbabwe Board**	The operations of the Authority shall, subject to this Act, be controlled and managed by a board to be known as the Data Protection Authority of Zimbabwe Board.
7	**Constitution of Board**	(1) Subject to subsection (2), the Board shall consist of not fewer than five members and not more than seven members appointed by the President after consultation with the Minister. (2) In appointing the members of the Board the President shall endeavour to secure that members are representative of groups or sectors of the community having an interest in human rights, information, and information/ communication technology, and, in particular, that at least three members are chosen for their experience or professional qualifications in the following fields or areas of competence (a) communications; (b) law, accountancy or administration.

8 **Terms of office and conditions of service of members**

(1) Subject to this Part, a member shall hold office for a period not exceeding three years.

(2) A member shall continue in office after the expiry of his term until he has been re-appointed or his successor has been appointed:

Provided that a member shall not hold office in terms of this subsection for longer than six months.

(3) Subject to section sixteen, a member shall hold office on such terms and conditions of service as the President may fix in relation to members generally.
(4) A retiring member is eligible for re-appointment as a member:
Provided that no member may be re-appointed for a third term in office.
(5) The terms and conditions of office of a member shall not, without the member's consent, be altered to his detriment during his tenure of office.

9 Disqualifications for appointment as member

(1) The President shall not appoint a person as a member and no person shall be qualified to hold office as a member who

(a) is neither a citizen of Zimbabwe nor permanently resident in Zimbabwe; or

(b) has a financial interest in any business connected with information communication technology or systems, or is married or connected to or associated with a person who has such an interest or is engaged in such an activity, or has any interest which will interfere with the person's impartial discharge of his duties as a member; or

(c) has, in terms of a law in force in any country

(i) been adjudged or otherwise declared insolvent or bankrupt and has not been rehabilitated or discharged; or

(ii) made an assignment to, or arrangement or composition with, his creditors which has not been rescinded or set aside; or

(d) has, within the period of five years immediately preceding the date of his proposed appointment, been convicted

(i) in Zimbabwe, of an offence; or

(ii) outside Zimbabwe, in respect of conduct which, if committed in Zimbabwe, would constitute an offence; and sentenced to a term of imprisonment imposed without the option of a fine, whether or not any portion has been suspended, and has not received a free pardon.

(2) A person who is —

(a) a member of Parliament; or

(b) a member of two or more other statutory bodies;

shall not be appointed as a member of the Board, nor shall he be qualified to hold office as a member.

(3) For the purposes of paragraph (b) of subsection (2) a person who is appointed to a council, board or other authority which is a statutory body or which is responsible for the administration of the affairs of a statutory body shall be regarded as a member of that statutory body.

10 **Vacation of office by member**

A member shall vacate his office and his office shall become vacant

(a) three months after the date upon which he gives notice in writing to the Minister of his intention to resign, or on the expiry of such other period of notice as he and the Minister may agree; or

(b) on the date he begins to serve a sentence of imprisonment imposed without the option of a fine

(i) in Zimbabwe, in respect of an offence; or

(ii) outside Zimbabwe, in respect of conduct which, if committed in Zimbabwe, would constitute an offence;

or

(c) if he becomes disqualified in terms of paragraph (a), (b) or (c) of subsection (1) of section eight, or in terms of subsection (2) of that section, to hold office as a member; or

(d) if he is required in terms of section ten to vacate his office.

11 **Dismissal or suspension of members**

(1) The President may require a member to vacate his office if the member-

(a) has, subject to subsection (3), been found to have conducted himself in a manner that renders him unsuitable as a member, including a contravention of section sixteen or subsection (2) of section twenty four; or

(b) has failed to comply with any term or condition of his office fixed by the President in terms of subsection (3) of section seven; or

(c) is mentally or physically incapable of efficiently carrying out his functions as a member; or

(d) has been absent without the permission of the Board from two consecutive meetings of the Board of which he was given at least seven days' notice, and there was no just cause for the member's absence.

(2) The President, on the recommendation of the Minister, may suspend a member

(a) whom he suspects on reasonable grounds of having been guilty of conduct referred to in paragraph (a) of subsection (1); or

(b) against whom criminal proceedings have been instituted for an offence in respect of which a sentence of imprisonment without the option of a fine may be imposed; and while that member is so suspended he shall not carry out any functions as a member.

(3) A member suspended in terms of paragraph (a) of subsection (2) shall be given notice in writing of the grounds for the suspension and may, within fourteen days of being so notified, make written representations to the Minister showing cause why no finding of misconduct rendering him unsuitable to be member of the Board should be made.

(4) The President, on the recommendation of the Minister, shall require a member suspended in terms of paragraph (a) of subsection (2) to vacate his office if

(a) no representations are made by the member in terms of subsection (3); or

(b) the President finds that, notwithstanding representations made in terms of subsection (3), the member is guilty of the misconduct alleged.

12 Access to the Authority

(1) Any person proving his/her identity has the right to address the Authority, free of charge, by himself/herself or by his/her lawyer or any other individual or legal person duly appointed.

13 Penalties

(1) The Authority may impose the following:

(a) a warning to a data controller failing to comply with the obligations of this Act.

Such warning shall be regarded as a sanction.

or

(b) a formal notice to comply to a data controller to cease the non-compliance within a given deadline. In case of urgency, this deadline may be limited to five days.

(2) Should the controller fail to comply with the notice served, the Authority may pronounce the following sanctions, after due hearing of the parties:

(a) Limitation or ceasing of the processing or suspension of authorization(s) issued, for a prescribed and/or

(b) Financial penalty of an amount not exceeding five thousand dollars (…);

(3) In case of serious and immediate violation of the individual rights and liberties, the Authority may rule, in summary proceedings:

(a) the limitation or ceasing of the personal data processing to the extent it relates to the violation;

or

(b) the temporary or definitive access to certain personal data processed;

or

(c) the temporary or definitive processing as not compliant with the provisions of this Act.

(4) The sanctions and decisions taken by the Authority may be subject to appeal through the judicial authorities.

14 Financial Provisions

(1) The funds of the Authority shall consist of
such moneys as may be payable to the Authority from moneys appropriated for the purpose by Act of Parliament; and such other moneys as may vest in or accrue to the Authority, whether in the course of its operations or otherwise.

PART III:

QUALITY OF THE DATA

15 **Quality of the data**

(1) The data controller shall ensure that personal 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; every reasonable step must be taken to ensure that data which is inaccurate or incomplete with respect to the purposes for which it is collected or for which it is further processed, is erased or rectified;

(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. The Authority shall establish appropriate safeguards for personal data retained longer than permitted above for historical, statistical or scientific research purposes.

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

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

PART IV:

GENERAL RULES ON THE PROCESSING OF PERSONAL DATA

16	**Generality**	(1) The data controller shall ensure that the processing of personal data is necessary and that the personal data is processed fairly and lawfully.
17	**Purpose**	(1) The data controller shall ensure that personal 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, 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.
18	**Non-sensitive data**	(1) The processing of non-sensitive personal 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) for compliance with an obligation to which the controller is subject by or by virtue of a law; or (c) in order to protect the vital interests of the data subject; or (d) for the performance of 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) for the promotion of the legitimate interests of the controller or the 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. (2) The Authority can specify the circumstances in which the condition stipulated under e) is considered as not having been met.
19	**Sensitive information**	(1) In relation to the processing of sensitive personal information, (a) The processing of sensitive data is prohibited unless the data subject has given consent in writing for such processing (b) This consent can be withdrawn by the data subject at any time and without any explanation and free of charge. (c) The Authority may determine the cases in which the prohibition to process the data referred to in this article 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."

(2) Paragraph (1) above 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/her consent or is not represented by his/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 organization with a political, philosophical, religious, health-insurance or trade-union purpose and on condition that the processing relates solely to the members of the organization 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 social security laws; or

(e) the processing is necessary, with appropriate guaranties, for the establishment, exercise or defense of legal claims; or

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

(g)

(i) the processing is necessary for the purposes of scientific research;

(ii) The Authority shall be entitled to specify the conditions under which such processing may be carried out; or

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

(3) (a) (i) Without prejudice to the application of sections 16 to 19, the processing of personal data relating to sex life is authorized if it is carried out by an association with a legal personality or by an organization of public interest whose main objective, according to its articles of association, is the evaluation, guidance and treatment of persons whose sexual conduct can be qualified as an offence, and who has been recognized and subsidized for the achievement of that objective by the competent public body for such processing,

(ii) the objective of which must consist of the evaluation, guidance and treatment of the persons referred to in this paragraph, and the processing of personal data, if it concerns sex life, relating only to the aforementioned persons, and

(iii) the competent public body referred to in (i) must grant a specific, individualized authorization, having received the opinion of the Authority.

(b) The authorization referred to in this paragraph shall specify the duration of the authorization, the conditions for supervision of the authorized association or organization by the competent public body, and the way in which the processing must be reported to the Authority.

20

Genetic data, biometric sensitive data and health data

(1)

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

(b) The consent referred to in previous paragraph (a) can be withdrawn by the data subject at any time without any motivation and free of charge;

(c) The Authority may determine the cases in which the prohibition to process the data referred to in this article cannot be lifted by the data subject's consent.

(2) Previous Paragraph (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 social 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/her consent or is not represented by his/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/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;

(3)

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

(b) Health-related personal data must be collected from the data subject.

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

(5) It may only be collected from other sources if paragraphs (3) and (4) above are complied with, and if such is necessary for the purposes of the processing, or if the data subject is incapable of providing the data.

(6) For the purposes of the processing of personal information affected by this Section. the health professional and his/her agents are subject to the duty of secrecy.

(7) In the scope of the above sections, the processing of genetic data, if they are processed for what they reveal or contain and personal data concerning health can be processed only if a unique patient identifier is given to the patient which is distinct from any other identification number, by the public authority established for this purpose.

(8) The association of this unique patient identifier with any other identifier which permits the identification of the data subject in the sense of section 19 is permissible only by the express authorization of the Authority.

The personal data of a child will be processed only in respect of the rules of representation pursuant to section 37.

PART V:

DUTIES OF THE DATA CONTROLLER AND DATA PROCESSOR

Disclosures when collecting data directly from the data subject

21. (1) When obtaining personal data directly from the data subject, the controller or the controller's representative shall concurrently 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/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 personal data relating to him/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 in 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;

(iii) the existence of the right to access and rectify the personal data relating to him/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.

Disclosures when not collecting data directly from the data subject

22. (1) Where the personal data is not collected from the data subject himself/herself, the controller or his/her representative must provide the data subject with at least the information set out below when recording the personal data or considering communication to a third party, and at the very latest when the data is first disclosed, 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/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 a right to object, by request and free of charge, to the intended processing of personal data relating to him/her, if it is obtained for the purposes of direct marketing; in that case, the data subject must be informed prior to the first disclosure of the personal 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 in 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 personal 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 previous paragraph (1) is not applicable 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) personal data is recorded or provided with a view to the application of a provision laid down by or by virtue of an act, decree or ordinance.

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

Authority to process

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

Security

24. (1)

(a) In order to safeguard the security of the personal data, the controller or his/her representative, if any, as well as the processor, must take the appropriate technical and organizational measures that are necessary to protect the personal data from negligent or unauthorized destruction, negligent loss, as well as from unauthorised alteration or access and any other unauthorized processing of the personal data.

(b) These measures 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..

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

(2) The data controller and his/her data processor, as the case may be, , shall appoint data processor(s)that provide sufficient guarantees regarding the technical and organizational security measures employed to protect the personal data associated with the processing undertaken and ensure strict adherence to such measures

(3)

(a) Any recourse to the data processor shall be governed by a contract or any other legal instrument which in legal terms, associates the data processor to the data controller.

(b) The contract or legislative act shall establish:

(i) that the data processor acts only under instruction of the data controller;

(ii) that the data processor is additionally, responsible for discharging the duties set out in previous paragraph (1) associated with the data processor's processing.

Security breach notification

25. (1) The data controller or his/her representative must notify the Authority, without any undue delay, of any security breach affecting personal data he/she processes on behalf of the data controller.

(2) The data processor must notify the data controller, without undue delay, of any security breach affecting personal data he/she processes on behalf of the data controller.

Obligation of notification to the Authority

26. (1)

(a) 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/her representative, if any, must notify the Authority.

(b) Any modification to the information provided according to Section 27 must be notified to the Authority.

(2) Previous Paragraph (1) does not apply to operations having the sole purpose of keeping a register that is intended to provide information to the public by virtue of an act, decree or ordinance and that is open to consultation either by the general public or by any person demonstrating a legitimate interest.

(3) The Authority can exempt certain categories from notification under this article 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)

(i) The data controller has appointed a data protection officer.

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

(iii) The data protection officer shall:

- be a person who shall have the qualifications required to perform his/her duties;
- keep a list of the processing carried out, which is immediately accessible to any person applying for access, and may not be sanctioned by his/her employer as a result of performing his/her duties.

(iv) He/she may apply to the Authority when he/she encounters difficulties in the performance of his/her duties.

(v) In case of non-compliance with the provisions of this law, the Authority shall order the data controller to carry out the formalities provided for in previous paragraph (1).

(vi) In case of breach of his/her duties, the representative shall be discharged from his/her functions upon the demand, or after consultation, of the Authority.

(vii) The Authority establishes the specific rules establishing the function of data protection officer.

(4) If exemption from the duty of notification has been granted for automatic processing in accordance with the previous paragraph, the data controller must disclose the items of information mentioned in section 27 to any person entitled to receive such information.

Content of the notification

27. (1) The notification must state, at least,:

(a) the date of notification and the act, decree, ordinance or regulatory instrument permitting the automatic processing, if any;

(b) the surname, first names and complete address or the name and registered offices of the controller and of his/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 personal 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 Chapter 6, section 3 above are adequate;

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

(m) the transfers of data to a third country as planned by the data controller;

(2) The Authority may establish other information which must 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 may inspect and assess the security and organizational measures prior to the commencement g of the processing or transfer.

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

Authorization

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

(2) Such authorization shall only be provided following receipt of notification from the data controller or from the data protection officer pursuant to sections 26 and 27.

Openness of the processing

29. (1)

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

(b) Any entry in the register must include the information mentioned in section 27.

(c) The register shall be available for consultation by all members of the public, in the manner determined by the Authority.

(2) In case of the processing 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 27.

Accountability

30. (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 to data subjects and to the Authority in the exercise of its powers.

PART VI:

RIGHTS OF THE DATA SUBJECT

Right of access

31. (1) Any data subject who proves his/her identity has the right to obtain, without any explanation and free of charge, from the controller or his/her representative, if any:

(a) information on whether or not data relating to him/her is being processed, as well as information regarding the purposes of the processing, the categories of data the processing relates to, and the categories of recipients the data is disclosed to;

(b) communication of the data being processed in an intelligible form, as well as of any available source of information;

(c) information about the basic logic involved in any automatic processing of data relating to him/her in case of automated decision making;

(d) information regarding his/her right of complaint under this chapter and his/her right to consult the register referred to in article 29 if necessary.

(2)

(a) To obtain such information the data subject shall submit a signed and dated request to the controller or the controller's appointed data protection officer.

(b) The Authority shall be entitled to specify further conditions for the application of this paragraph (2) (a).

(3)

(a) Where sensitive personal data is processed for the purpose of scientific research and there is no evident risk of infringement of the data subject's right to protection of his/her privacy and the data being used to impose measures or take decisions with regard to an individual, informing the data subject may be postponed until the moment the research is concluded, but only to the extent that informing the data subject would significantly prejudice the research.

(b) In this case the data subject must have given to the data controller his/her previous written consent to the processing of personal data relating to him/her for scientific research purposes and to postponing, for that reason, the moment at which he is informed.

(4) The waiver of any charge pursuant to Paragraph (1) above may be refused by the data controller in case of misuse of the request by the data subject.

(5) The data controller's decision may be the subject of a complaint by the data subject to the Authority in accordance with section 4.

Right of rectification, deletion and temporary limitation of access

32. (1)

(a) The data subject has the right, as the case may be and free of charge, of rectification, deletion of the personal data relating to him/her or temporary limitation of access to these personal data if the processing is not compliant with this Act, especially if the personal data concerned is not complete or inaccurate.

(b) Any person also has the right to obtain free of charge the deletion of, or prohibition of the use of, all personal data relating to him/her that is incomplete or irrelevant to the purpose of the processing, or where the recording, disclosure or storage of the data is prohibited, or where it has been stored for longer than the authorized retention period..

(2) The data subject has the right to obtain from the controller notification of all third parties to whom their personal data has been disclosed as well as rectification, deletion or temporary limitation pursuant to paragraph (1) unless this proves impossible or involves a disproportionate effort.

(3) The condition that the fulfillment of such right shall be free of charge pursuant paragraph (1) may be refused by the data controller in the case of misuse of the request by the data subject.

(4) The data controller's decision may be the subject of a complaint by the data subject to the Authority in accordance with Article 6.

Right of objection

33. (1) The data subject has the right:

(a)

(i) to object at any time and free of charge, on compelling legitimate grounds relating to his/her particular situation (such as judicial proceeding), to the processing of data relating to him/her, unless the lawfulness of the processing is based on the reasons referred to in Articles 14 (1) (a), 14 (1) (b), 15 (2) (a), 15 (2) (d), 15 (2) (j), 16 (2) (a), 16 (2) (b) and 17 (2) (d).

(ii) Where there is a justified objection, the processing in question may no longer involve such data;

or

(b) to be informed before personal data is disclosed for the first time to third parties or before they are used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosure or use.

(2) The waiver of any charge pursuant to paragraph (1) may be refused by the controller in the case of misuse of the request by the data subject.

(3) The data controller's decision may be the subject of a complaint by the data subject to the Authority in accordance with Article 6.

Delays

34. The data controller respond to the request of the data subject within 45 days. If not, a complaint may be addressed to the Authority.

Further Regulation

35. The Authority shall consult with the Minister for the passing of regulations relating to the exercise of the right referred to in Articles 31 to 33.

Decision taken purely on the basis of automatic data processing

36. (1) A decision having legal effects on a person or significantly affecting him/her, must not be taken purely on the basis of automatic data processing with the aim of assessing certain aspects of his/her personality.

(2) The prohibition referred to in paragraph (1) is not applicable if the decision is taken in the context of an agreement or is based on a provision established by or by virtue of law. That agreement or provision must contain suitable measures to safeguard the legitimate interests of the data subject defined by his/her national law or international convention. The latter person must be given at least the chance to defend his/her point of view.

Representation of the data subject who is a child

37. (1) If the data subject is a child, his/her rights pursuant this law may be exercised by his/her parents or legal guardian unless the law states that the child may act by himself without being represented by his/her parents or legal guardian.

(2) Following his/her age and capability, he/she shall be entitled to independently exercise of his/her rights.

Representation of physically, mentally or legally incapacitated data subjects

38. (1) A data subject who is not subject to Section 37 and who is physically, mentally or legally incapable of exercising the rights given by this Act, may exercise such rights through a spouse, partner , or any such person as legally declared by the law as being the guardian.

b. Incapacity referred to in a above shall be proved by a physician or a person legally competent to do so.

(2)

(a) If such person referred to in (1) above, does not accept the charge or is in default, a specific guardian designed by the competent Court will exercise the rights of the data subject.

(b) This is also valid in the case of conflict between two or more people mentioned in paragraph 1.

(3) The data subject shall be entitled to the exercise of his/her rights to the furthest extent taking into account his/her capability.

PART VII

RECOURSE TO THE JUDICIAL AUTHORITY

Recourse to the judicial authority

39. Subject to the exhaustion of the appeal offered through the Authority under this law, the data subject shall be entitled to pursue legal appeals with the relevant judicial authorities.

PART VIII

SANCTIONS

Penalties

40. (1) Any member, permanent of substitute, personnel, consultant, contractor or other member of staff of the Authority or any expert who has violated the obligation of secrecy referred to in this Act shall be shall be guilty of an offence and liable to a fine not exceeding level seven or to imprisonment for a period not exceeding two years or to both such fine and such imprisonment.

(1) Any data controller, his/her representative, agent or assignee who:
(a) does not comply with the obligations laid down in Articles 24 to 25
(b) who processes personal data in violation of the conditions imposed by Sections 11 (1), 12 and 13
(c) who processes data in violation of Sections 15 to 19
(d) who knowingly communicates incorrect or incomplete information
(e) who having started, managed, continued to manage or terminated the automatic processing of personal data does so without meeting the requirements of Section 26
(f) who in violation of Section29 (2), refuses to communicate to the Authority information requested who transfers personal data or has personal data transferred to a country outside the SADC included in the list referred to in Article 44 (2), or any person who authorizes such transfers despite the requirements of Article 45;

shall be guilty of an offence and liable to a fine not exceeding level eleven or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment. (taken from Postal and Telecommunications Act 12:05)

(3) A fine of (…) to (…) shall be imposed on:

(a) any controller, his/her representative, agent or assignee processing personal data in violation of the conditions imposed by Articles 11 (1), 12 and 13;

(b) any controller, his/her representative, agent or assignee processing personal data in cases other than those in Article 14;

(c) any controller, his/her representative, agent or assignee processing personal data in violation of Articles 15 to 19;

(d) any controller, his/her representative, agent or assignee having failed to communicate the information referred to in article 31 (1) within (…) days of receipt of the request, or who knowingly communicates incorrect or incomplete information;

(e) any person who resorts to acts of violence, force, threats, donations or promises with the purpose of forcing another person into disclosing information that was obtained through the exercise of the right defined in Article 31 (1), or with the purpose of obtaining the other person's consent for the processing of personal data relating to that person; (b) any controller, his/her representative, agent or assignee processing personal data in cases other than those in Article 14;

(f) any controller, his/her representative, agent or assignee having started, managed, continued to manage or terminated the automatic processing of personal data without meeting the requirements of Article 26;

(g) any controller, his/her representative, agent or assignee having communicated incomplete or incorrect information in the notifications imposed by Article 27;

(h) any controller, his/her representative, agent or assignee who, in violation of article 29 (2), refuses to communicate to the Authority information requested;

(i) any person who transfers personal data or has personal data transferred to a country outside Zimbabwe included in the list referred to in Article 44 (2), or any person who authorizes such transfers despite the requirements of Article 45;

(j) any person who prevents the Authority, its members or its experts from proceeding with the inquiry referred to in Article 4.

(5)

(a) Upon conviction for any of the offences described in this article, the judge can pronounce the seizure of the media containing the personal data to which the offence relates, such as manual filing systems, magnetic discs or magnetic tapes, except for computers or any other equipment, or he can order the deletion of the data.

(b) Seizure or deletion can also be ordered even if the media containing the personal data do not belong to the person convicted.

(c) The objects seized shall be destroyed when the judgment has become final.

(6) The present article is not an impeachment to any measure of leniency set by law as the suspension or the suspended sentence except for the sentences set in Paragraphs (4) and (5) above.

(7) Without prejudice to the revocation of competences laid down in particular provisions, the Court can, upon conviction for an offence mentioned in this article, impose a prohibition to manage any processing of personal data, directly or through an intermediary, for a maximum of three (3) years.

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

PART IX

LIMITATIONS

Limitations

41. (1) This Act does not apply to the processing of personal data by a natural person in the course of purely personal or household activities.

(2) Article 11 (1) (c), Articles 15, 18, 21, 22, 26, 31 and 32 and Part X shall not apply to processing of personal data carried out for the sole purpose of literary and artistic expression;

PART X

TRANSBORDER FLOW

To a Member State which has transposed the SADC Model Law

42. (1) Without prejudice to Articles 11, 12, 13 and 17, personal data shall only be transferred to recipients,

(a) if the recipient establishes that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public body, or if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced.

(b) The controller shall be required to verify the competence of the recipient and to make a provisional evaluation of the necessity for the transfer of the data. If doubts arise as to this necessity, the controller shall seek further information from the recipient.

(c) The recipient shall ensure that the necessity for the transfer of the data can be subsequently verified.

(c) The recipient shall process the personal data only for the purposes for which they were transmitted

To a Member state which has not transposed the SADC Model Law or to a non SADC Member State

43. (1)

(a) Personal data shall only be transferred to recipients, other than Member States of the SADC, which are not subject to national law adopted pursuant to the SADC Model Law, if an adequate level of protection is ensured in the country of the recipient or within the recipient international organization and the data are transferred solely to allow tasks covered by the competence of the controller to be carried out.

(b) The adequacy of the level of protection afforded by the third country or international organization in question shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be 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 organization, the rules of law, both general and sectorial, in force in the third country or international organization in question and the professional rules and security measures which are complied with in that third country or international organization.

(2) The Authority shall lay down the categories of processing operations for which and the circumstances in which the transfer of personal data to countries outside the SADC is not authorized.

Transfer to a country outside the SADC which does not assure an adequate level of protection

44. (1) By way of derogation from section 43, a transfer or a set of transfers of personal data to a country outside the SADC 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/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.

(2) Without prejudice to the provisions of the previous paragraph, the Authority may authorize a transfer or a set of transfers of personal data to a country outside the SADC which does not ensure an adequate level of protection, if the controller ensures adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, and regarding the exercise of the corresponding rights; such safeguards can result from appropriate contractual clauses in particular.

PART XI

CODE OF CONDUCT

Code of Conduct

45. (1) The Authority shall 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 drawn up draft national codes or have the intention of amending or extending existing national codes to be able 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 drafts submitted to it are in accordance with this Act. If it sees fit, the Authority shall seek the views of affected data subjects or their representatives.

PART XII

WHISTLEBLOWING

Whistleblowing

46. (1)

(a) The Authority shall establish rules giving the authorization for and governing the whistleblowing system.

(b) These rules must preserve:

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

(ii) the principles related to the proportionality as the limitation of the scope, accuracy of the data which will be processed;

(iii) the principle of openness with delivering an adequate collective and individual information on:

- the scope and purpose of the whistleblowing;
- the processing of reporting;
- the consequences of the justified and unjustified reporting;
- the way of exercising the rights of access, to rectification, deletion as well as the competent authority to which a request can be made; and
- the third party which may receive personal data concerning the informer and the person who is implicated in the scope of the processing of the reporting (for example the internal audit service if the "manager of the reporting" needs to verify some points),

the person who is implicated shall be informed as soon as possible by the "manager of the reporting" of the existence of the reporting and about the facts which he/he is accused for in order to exercise the rights established in this Act; and

the information of the person who is implicated may be postponed in exceptional circumstances (e.g.: risk of proof destruction).

(iv) the technical and organizational rules;

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

(vi) the rules of notification to the Authority.