THE DATA PROTECTION BILL, 2020

(Bill No……of 2020)

(To be presented by the Minister for Information Communications and Technology)

MEMORANDUM OF OBJECTS AND REASONS

The object of this Bill is to provide for -

(a) the collection and processing of personal data;
(b) the protection of personal data;
(c) disclosure of personal data for legitimate purposes;
(d) rights of access to and correction of personal data; and
(e) incidental matters.

SIFISO.M.M. KHUMALO

ATTORNEY-GENERAL

A BILL
ENTITLED

AN ACT to provide for the collection, processing, disclosure and protection of personal data; balancing competing values of personal information privacy and sector-specific laws and other related matters.

ENACTED by the King and the Parliament of Eswatini

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY PROVISIONS

PART II

RESPONSIBILITIES OF THE COMMISSION

PART III

PROCESSING OF PERSONAL INFORMATION

PART IV

EXEMPTIONS FROM PROTECTION ON PROCESSING OF PERSONAL INFORMATION

PART VIII

MISCELLANEOUS PROVISIONS

PART I

PRELIMINARY

Citation and Commencement

1. (1) This Act may be cited as the Data Protection Act, 2020.

(2) This Act shall come into operation on the date of publication in the Gazette.

Interpretation

2. In this Act, unless the context otherwise requires –

“authorization” means a licence or individual right of use that a person may

hold or be granted under any law administered by the Commission;

“biometric” means a technique of personal identification that is based on physical characteristics including fingerprinting, DNA analysis, retinal scanning and voice recognition;

“child” has the same meaning ascribed in the Children’s Protection and Welfare Act, 2012;

“code of conduct” means codes of conduct approved by the Commission and includes industry codes of conduct applicable to a data controller and approved by the Commission;

“Commission” means the Eswatini Communications Commission, established under the Eswatini Communications Commission Act, 2013;

“Constitution” means the Constitution of the Kingdom of Eswatini, 2005;

“data” refers to all representations of information notwithstanding format or medium;

“data controller” means a public or private body which or any other person designated by law, who alone or together with others, determines the purpose of and means for processing personal information, regardless of whether or not such data is processed by that party or by a data processor on its behalf, where the purpose and means of processing are determined by law;

“data processor” refers to a natural or legal person, or public body which processes personal information for and on behalf of a data controller and under the instructions of a data controller, and excludes persons who are authorised to process data under the direct authority of a data controller;

“Data Protection Officer; means a person appointed by a data controller

charged with ensuring compliance with this Act;

“data subject” means a person who is the subject of the processing of personal information and who is identified or identifiable;

“de-identify or de-identified” in relation to personal information of a data subject, means to delete any information that -

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; and

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject;

“explicit consent” means any voluntary, specific and informed consent communicated expressly by spoken or written words in terms of which a data subject agrees to the processing of personal information relating to a data subject;

“filing system” means a set or collection of personal data records, structured either by reference to individuals or criteria relating to individuals, in a way that specific information relating to a particular individual is readily accessible;

“identifiable person” means an individual who can be identified, directly or indirectly, in particular, by reference to an identification number or to one or more factors specific to one’s physical, physiological, mental, economic, cultural or social identity taking into account all the means reasonably likely to be used either by the controller or by any other person to identify the said person;

“implicit consent” means consent that is inferred from signs, actions or facts, or by inaction or silence;

“Minister” means the minister responsible for Information

Communications and Technology;

“personal data or information” means information about an identifiable individual that is recorded in any form, including without restricting the generality of the foregoing -

(a) information relating to the race, national or ethnic origin, religion, age or marital status of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;

(c) any identifying number, symbol or other particular assigned to the individual;

(d) the address, fingerprints or blood type of the individual;

(e) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual;

(f) correspondence sent to a data controller by the individual that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence; and

(g) the views or opinions of any other person about the individual.

“processing” means an operation or activity or any set of operations, whether or not by automatic means relating to –

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as blocking, degradation, erasure, or destruction, of information;

"public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;

"record" means any recorded information in the possession or under the control of a data controller -

(a) whether or not it was created by the data controller or when it came into existence;

(b) regardless of form or medium, including –

(i) writing on any material;

(ii) information produced, recorded or stored by means of any tape -recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so-produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing; or

(v) photograph, film, negative, tape, or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

"re-identify or re-identified" in relation to personal information of a data subject, means to resurrect any information that has been de-identified that –

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject.

"sensitive personal information" means –

(a) genetic data, data related to children, data related to offences, criminal sentences or security measure, biometric data as well as, if it is processed for what it reveals, personal information revealing racial or ethnic origin, political opinions or affiliations, religious or philosophical beliefs, affiliation, trade-union membership, gender and data concerning health or sex life; or

(b) any personal information otherwise considered by the laws of Eswatini as presenting a major risk to the rights and interests of the data subject, in particular unlawful or arbitrary discrimination;

"trans-border flow" means any international cross border flows of personal information by means of electronic transmission or any transmission means including data transmission by satellite; and

"whistleblowing" means allowing individuals to report the behaviour or conduct of any person which, is considered to be contrary to a law or regulation or fundamental rules.

Application

3. This Act applies to –

(a) a data controller, whether or not domiciled or having its principal place of business in Eswatini, who uses automated or non-

automated means in Eswatini for forwarding personal information; and

(b) processing of personal information performed wholly or partly by automated means.

Exemptions

4. This Act does not apply to the processing of personal information –

(a) in the course of a purely personal or household activity;

(b) which has been de-identified to the extent that it cannot be re-identified;

(c) by or on behalf of the State and involves national security and defence or public safety;

(d) solely for journalistic purposes or the purposes of artistic or literary expression, where the artistic or literary expression are necessary to reconcile the right to privacy with the rules governing freedom of expression; or

(e) which has been exempted under this Act.

PART II

RESPONSIBILITIES OF THE COMMISSION

Functions of Commission

5. (1) The Commission shall –

(a) administer this Act and protect the respective rights of information privacy provided for under this Act or any

other law;

(b) engage in ensuring that the processing of personal data by the controller complies with this Act;

(c) promote an understanding and acceptance of information protection principles through education and public awareness;

(d) make public statements in relation to any matter affecting protection of personal information;

(e) monitor and enforce compliance with the provisions of this Act by public and private bodies;

(f) undertake research and monitor developments in information processing and computer technology to ensure that any adverse effects of such developments on protection of personal information of data subjects are minimised;

(g) examine any proposed policy or legislation which may affect the protection of personal information;

(h) report with or without request to Parliament from time to time, on any matter affecting the protection of personal information of a data subject, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to personal information;

(i) conduct from time to time, audits of personal information maintained by a data controller for the purpose of ascertaining whether or not the information is maintained according to the information protection principles;

(j) monitor constantly, the use of unique identifiers of data subjects;

(k) maintain, publish and provide copies of registers as required under this Act;

(l) receive and invite representations from members of the public on any matter provided for under this Act;

(m) consult and cooperate with other persons and bodies including international data protection authorities concerned with the protection of personal information;

(n) participate in any international and regional cooperation and negotiation on matters of data protection impacting Eswatini;

(o advise Parliament or a public or private body on the obligations of that public or private body under this Act;

(p) receive, investigate and resolve complaints on alleged violations of the provisions of this Act, and report the findings and decisions to the complainants;

(q) receive complaints or reports of violations of individual rights and liberties under this Act and refer such complaints and reports to the Human Rights and Public Administration Commission for investigation and determination;

(r) report to Parliament from time to time on the desirability of the acceptance by Eswatini, of any international instrument relating to the protection of personal information;

(s) issue, approve, amend or revoke codes of conduct;

(t) make and issue Guidelines to assist public or private bodies to develop codes of conduct or to apply codes of conduct;

(u) impose administrative sanctions which may be punitive, depending on the facts of the matter such as the cancelling of the authorization of processing of personal information, fines or awarding of damages to the benefit of the injured data subject in the case of violation of the provisions of this Act;

(v) establish mechanisms of cooperation with other authorities or other data protection authorities from other countries, for purposes of resolving cross-border disputes pertaining to data protection and information privacy;

(w) review a decision made under an approved code of conduct;

(x) exercise and perform such other functions or powers conferred by this Act; and

(y) make such decisions and authorizations as may be necessary in carrying out the functions of the Commission.

(3) The Commission may, from time to time, in the public interest or in the legitimate interests of any person or body of persons, publish reports relating to the exercise of the functions of the Commission under this Act or to any case investigated by the Commission.

Powers of the Commission to impose sanctions

6. (1) The Commission may issue -

(a) a warning to a data controller who fails to comply with the obligations of this Act; or

(b) a formal notice calling upon a data controller to comply within a specified period.

(2) A warning and notice issued in term of subsection (1) shall be served on the data controller by the Commission.

(3) Where the controller fails to comply with a notice issued in terms of subsection (1) (b), the Commission may -

(a) limit, suspend or terminate the authorization of a data collector to process personal information, issued under this Act, or

(b) impose an administrative fine not exceeding One Hundred Million Emalangeni (E100 000 000) or 5 percentage (%) of the annual turnover of the data controller.

(4) Where a person or body or persons fails to comply with the provisions of this Act the Commission may -

(a) cancel or suspend the authorization to process personal information;

(b) impose a fine against that person or body or persons; or

(c) order that person or body or persons compensate to the benefit of an aggrieved person or data subject.

Protection of Commission

7. The Commission, its employees or any person acting on behalf of or under the direction of the Commission shall not be civilly or criminally liable for anything done in good faith in the exercise or performance of any power, duty or function of the Commission in terms of this Act.

Confidentiality

8. A person acting on behalf of or under the direction of the Commission shall treat as confidential, personal information which comes to their knowledge, except where the communication of such information is required by law or in the proper performance of their duties.

PART III

PROCESSING OF PERSONAL INFORMATION

Processing of personal information

9. (1) The processing of personal information shall be processed and kept in –

(a) a filing cabinet; and or

(b) electronic form.

(2) Personal information shall be processed if –

(a) the data subject provides explicit consent to the processing;

(b) processing is necessary for the conclusion or performance of a contract to which the data subject is a party;

(c) processing is necessary for compliance with a legal obligation to which the data controller is subject;

(d) processing is necessary to protect the legitimate interests of the data subject;

(e) processing is necessary for the proper performance of public law duty by a public body; or

(f) processing is necessary for pursuing the legitimate interests of the data controller or of a third party to whom the information is supplied.

(3) A data subject, may, on compelling legitimate grounds, make a written objection to the processing of data relating to that data subject to the Commission on the grounds that the processing does not comply with the conditions listed in subsection (1) and where the objection is upheld by the Commission, the data controller shall not process the data.

(4) Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

Collection of personal information from data subject

10. Personal information shall be collected except where –

(a) the information is contained in a public record or has deliberately been made public by the data subject;

(b) the data subject has consented to the collection of the information from another source;

(c) collection of the information from another source would not prejudice a legitimate interest of the data subject;

(d) collection of the information from another source is necessary –

(i) to avoid prejudice to the maintenance or enforcement of law and order;

(ii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

(iii) in the legitimate interests of national security; or

(iv) to maintain the legitimate interests of the data controller or of a third party to whom the information is supplied;

(e) compliance would prejudice a lawful purpose of the collection of the information; or

(f) compliance is not reasonably practicable in the circumstances of the particular case.

Collection of personal information by data controller

11. (1) Where personal information is collected by the data controller directly from the data subject, the data controller shall take reasonable and practicable steps to ensure that the data subject is aware of –

(a) the information being collected;

(b) the name and address of the data controller;

(c) the purpose for which the information is being collected;

(d) whether or not the supply of the information by the data subject is mandatory;

(e) the consequences of failure to provide the information;

(f) any law authorising or requiring the collection of the information; and

(g) any further information which is necessary having regard to the specific circumstances, such as the –

(i) recipient or category of recipients of the information;

(ii) nature or category of the information; and

(iii) existence of the right of access to and the right to rectify the information collected.

(2) The steps referred to in subsection (1) shall be taken –

(a) before the information is collected, unless the data subject is already aware of the information under subsection (1); or

(b) in any other case, as soon as reasonably practicable after it has been collected.

(3) A data controller which has previously taken the steps referred to in subsection (1) shall be deemed to be in compliance with subsection (1) in relation to the subsequent collection of information or information of the same kind from the data subject if the purpose of collection of the information is unchanged.

(4) A data controller may not comply with subsection (1) where –

(a) the data subject has provided consent for non-compliance with that subsection;

(b) non-compliance with that subsection would not prejudice the legitimate interests of the data subject as set out under this Act;

(c) non-compliance with that subsection is necessary –

(i) to avoid prejudice to the maintenance or enforcement of law and order;

(ii) to enforce a law imposing a pecuniary penalty;

(iii) to enforce legislation concerning the collection of revenue by the state;

(iv) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated, or are in the interests of national security;

(d) compliance with subsection (1) would prejudice a lawful

purpose of the collection of the personal information;

(e) compliance with subsection (1) is not reasonably practicable in the circumstances of the particular case; or

(f) the information shall –

(i) not be used in a form in which the data subject may be identified; or

(ii) be used for historical, statistical or research purposes.

Purpose specification and further processing limitation

12. (1) Personal data shall be collected for specified, explicit and legitimate purposes and shall not be further processed in a way incompatible with those purposes.

(2) The further processing of personal information shall be compatible with the purposes of collection if –

(a) the data subject has consented to the further processing of the information;

(b) the information is available in public records or has deliberately been made public by the data subject;

(c) further processing is necessary –

(i) to avoid prejudice to the maintenance of the law or enforcement of law and order;

(ii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

(iii) in the legitimate interests of national security;

(d) the further processing of the information is necessary to

prevent or mitigate a serious and imminent threat to –

(i) public health and safety; or

(ii) the life and health of the data subject or another individual;

(e) The information is used for historical, statistical or research purposes and the data controller has established appropriate safeguards against the personal data being used for any other purposes.

Retention of records

13. (1) Subject to subsections (2) and (3), records of personal information shall not be retained any longer than a prescribed period unless –

(a) retention of the record is required or authorised by law;

(b) the data controller reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties; or

(d) the data subject has consented to the retention of the record.

(2) Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes and the data controller has established appropriate safeguards against the personal data being used for any other purposes.

(3) A data controller which or who has used a record of personal information of a data subject to make a decision about the data subject shall –

(a) retain the record for such period as may be required or prescribed by law or a code of conduct; or

(b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

(4) A data controller shall destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the data controller is no longer authorised to retain the record in terms of subsection (1) or (2).

(5) The destruction or deletion of a record of personal information in terms of subsection (4) shall be done in a manner that prevents its reconstruction.

Security measures on integrity of personal information

14. (1) A data controller shall secure the integrity of personal information in its possession or under its control by taking appropriate, reasonable technical and administrative measures to prevent –

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the data controller shall take reasonable measures to –

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The data controller shall have due regard to generally accepted information security practices and procedures or professional rules and regulations which may apply generally or be required in the specific industry.

Processing of information by a data processor on behalf of data controller

15. A data processor or anyone processing personal information on behalf of a data controller shall –

(a) process such information only with the knowledge or authorisation of the data controller; and

(b) treat personal information which comes to their knowledge as confidential and shall not disclose it, unless required by law or in the course of the performance of their duties.

Security measures for information processed by data processor

16. (1) A data controller shall ensure that a data processor which processes personal information for or on behalf of the data controller establishes and maintains the security measures referred to in this Act.

(2) The processing of personal information for a data controller by a data processor on behalf of the data controller shall be governed by a written contract between the data processor and the data controller, which requires the data processor to establish and maintain confidentiality and security measures to ensure the integrity of the personal information.

(3) Where the data processor is not domiciled or does not have its principal place of business in Eswatini, the data controller shall take reasonable steps to ensure that the data processor complies with the laws relating to the protection of personal information of the territory in which the data processor is domiciled.

Notification of security compromise

17. (1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by an unauthorised person, the data controller, or any other third party processing personal information under the authority of a data controller, shall notify -

(a) the Commission; and

(b) the data subject, unless the identity of such data subject cannot be established.

(2) The notification referred to in subsection (1) shall be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the information system of the data controller.

(3) The data controller shall delay notification to the data subject where the Police or the Commission determines that notification will

impede a criminal investigation.

(4) The notification to a data subject referred to in subsection (1) shall be in writing and communicated to the data subject in one of the following ways –

(a) mailed to the last known physical or postal address of the data subject;

(b) sent by e-mail to the last known e-mail address data subject;

(c) placed in a prominent position on the website of the party responsible for notification;

(d) published in the news media; or

(e) as may be directed by the Commission.

(5) A person making notification shall ensure that the notification provides sufficient information to allow the data subject to take protective measures against potential consequences of the compromise, including, if known to the data controller, the identity of the unauthorised person who may have accessed or acquired the personal information.

(6) The Commission may direct a data controller to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, where the Commission has reasonable grounds to believe that the public would protect a data subject who may be affected by the compromise.

Quality of information

18. (1) A person who is responsible for collecting and processing of personal information shall take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and kept up

to date where necessary.

(2) In taking the steps referred to in subsection (1), the party responsible for collecting and processing of personal information shall have regard to the purpose for which personal information is collected and processed.

Access to and challenging of personal information

19. (1) A data subject who provides adequate proof of identity, shall have a right to request –

(a) a data controller to confirm, free of charge, whether or not the data controller holds personal information about the data subject; and

(b) from a data controller, personal information about the data subject held by the data controller, including information about the identity of all third parties who have or have had, access to the information –

(i) within a prescribed time;

(ii) at a prescribed fee;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

(2) Where the data controller denies a data subject a request made in terms of subsection (1) the data subject shall be entitled to be given written reasons for the denial.

(3) A data subject shall have a right to challenge the written reasons for denial or requests made in terms of subsection (1).

(4) If, in accordance with subsection (1) (b), personal information is communicated to a data subject, the data subject shall be advised of the

right in terms of this Act to challenge the correctness of the information.

Correction of personal information

20. (1) A data subject shall, free of charge have a right to challenge the correctness of information by requesting that a data controller –

(a) corrects or deletes personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(b) destroys or deletes a record of personal information about the data subject that the data controller is no longer authorised to retain.

(2) A data controller shall, on receipt of a request in terms of subsection (1), take reasonable steps to investigate the challenging of personal information lodged and –

(a) correct, destroy or delete the information; or

(b) provide that data subject, with credible evidence in support of the correctness of the information.

(3) Where credible evidence has been provided under subsection (2)(b), the data subject may apply to the Commission to investigate the disputed information.

(4) Where the data controller has taken steps under subsection (2)(a) that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the data controller shall, within seven (7) working days inform each person, body or data controller to whom the personal information has been disclosed of those steps.

(5) The data controller shall notify a data subject who has made a request in terms of subsection (1), of the outcome of the request within a period of fourteen (14) days of the making of the request.

Data controller to give effect to principles of this Act

21. The data controller shall –

(a) ensure that the principles set out under this Act and all the measures that give effect to the principles are complied with; and

(b) have the necessary internal mechanisms in place for demonstrating compliance with the principles of this Act to both data subjects and the Commission in the exercise of its powers.

Prohibition against processing of sensitive personal information

22. Unless specifically permitted under this Act, a data controller shall not process sensitive personal information.

PART IV

EXEMPTIONS FROM PROTECTION ON PROCESSING OF PERSONAL INFORMATION

Exemption on spiritual, religious or philosophical beliefs of data subject

23. (1) The exemption on processing personal information of the spiritual, religious or philosophical beliefs of a data subject shall not apply if the processing is carried out by –

(a) spiritual or religious organizations; or

(b) independent sections of those organizations.

(2) Subsection (1)(a) shall not apply where the information concerns a data subject belonging to the organization mentioned in paragraph (a).

Exemption on race of data subject

24. (1) The prohibition on processing personal information concerning the race of a data subject shall not apply if the processing is carried out to –

(a) identify a data subject and only when this is essential for that purpose; and

(b) comply with the law.

(2) In the cases referred to under subsection (1), personal information shall not be supplied to third parties without the consent of the data subject.

Exemption on trade union membership of data subject

25. (1) The prohibition on processing personal information on the trade union membership of a data subject, shall not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs, where the processing is necessary to achieve the aims of the trade union or trade union federation.

(2) In the cases referred to under subsection (1), personal information shall not be supplied to third parties without the consent of the data subject.

Exemption on political affiliation of data subject

26. (1) The prohibition on processing personal information concerning a political affiliation of a data subject, shall not apply to processing by an institution founded on political principles of the personal information of their members or employees, or other personal belonging to the institution if such processing is necessary to achieve the aims or principles of the institution.

(2) In the cases under subsection (1), personal information shall not be supplied to third parties without the consent of the data subject.

Exemption on health or sexual life of data subject

27. (1) The prohibition on processing personal information on health or sexual life of a data subject, shall not apply to the processing by –

(a) medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;

(b) insurance companies, medical aid scheme administrators, and managed healthcare organisations where such processing is necessary for –

(i) assessing the risk to be insured by the insurance company or covered by the medical aid scheme and the data subject has not objected to the processing;

(ii) the performance of an insurance or medical aid agreement; or

(iii) the enforcement of any contractual rights and obligations;

(c) schools, where such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sexual life;

(d) institutions or probation, child protection or guardianship, where such processing is necessary for the performance of their legal duties;

(e) correctional institution or facility where such processing is necessary in connection with the implementation of prison sentences or detention measures; or

(f) administrative bodies, pension funds, employers or institutions working for them, where such processing is necessary for –

(i) the implementation of the provisions of the law, pension regulations or collective agreements which create rights dependent on health or sexual life of the data subject; or

(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) In cases under subsection (1), the information shall be processed by a data controller subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the data controller and the data subject.

(3) A data controller that is permitted to process information on a data subject's health or sexual life in terms of this section and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, shall treat the information as confidential, unless the

responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information.

(4) The prohibition on processing any of the categories of personal information shall not apply where it is necessary to supplement the processing of personal information on a data subject's health, with a view to the proper treatment or care of the data subject.

(5) Personal information concerning inherited characteristics shall not be processed in respect of a data subject from whom the information concerned has been obtained unless –

(a) a serious medical interest prevails; or

(b) the processing is necessary for the purpose of scientific research or statistics.

(6) The Commission may prescribe more detailed rules concerning the application of subsection 1(b) and (f).

Exemption on criminal behaviour of data subject

28. (1) The prohibition on processing of personal information on criminal behaviour of a data subject, shall not apply where the processing is carried out by a body charged by law with applying criminal law or by a data controller who has obtained that information in accordance with this Act.

(2) The prohibition shall not apply to a data controller who processes the information for their own lawful purposes to –

(a) assess an application by a data subject in order to take a decision about, or provide a service to that data subject; or

(b) protect their legitimate interests in relation to criminal

offences which have been or can reasonably be expected to be committed against them or against persons in their service.

(3) The processing of information concerning personnel in the service of the data controller shall take place in accordance with the rules established in compliance with the labour laws.

(4) The prohibition on processing any of the categories of personal information referred to in this Part, shall not apply where such processing is necessary to supplement the processing of information on criminal behaviour permitted under this section.

General exemption on sensitive personal information

29. Without prejudice to Sections 23 to 28, the prohibition on processing sensitive personal information shall not apply where –

(a) processing is carried out with prior parental consent where the data subject is a child and is subject to parental control in terms of the law;

(b) the processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law;

(d) the Commission has granted authority in terms of section 30 for processing in the public interest, and appropriate guarantees have been put in place in law to protect the data subject's privacy;

(e) processing is carried out with the consent of the data subject; or

(f) the information has deliberately been made public by the data subject.

Authorisation by the Commission

30. (1) The Commission may authorise a data controller to process personal information, where the Commission is satisfied that, in the circumstances of the case -

(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or

(b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.

(2) The public interest referred to in subsection (1)(a) includes –

(a) the legitimate interests of State security;

(b) the prevention, detection and prosecution of offences;

(c) important economic and financial interests of the State or a public body;

(d) fostering compliance with legal provisions established in the interests referred to under paragraphs (b) and (c);

(e) historical, statistical or research purposes, and the data controller has established appropriate safeguards against the personal data being used for any other purposes or;

(f) the legitimate interests of individual or public, relating to health or protection of life or environmental safety

(3) The Commission may impose reasonable conditions in respect of any authorisation issued under subsection (1).

Exemption for processing of personal data for historical, statistical and research purposes

31. (1) The processing of personal information for historical, statistical and research purposes is exempt from all of the information protection principles except –

(a) the principle regulating security safeguards; or

(b) the principle regulating information quality.

(2) The data controller shall establish appropriate safeguards against the use of the data for any other purpose.

PART V

TRANS-BORDER FLOW OF PERSONAL INFORMATION OUTSIDE ESWATINI

Transfer of personal information within SADC Member States

32. (1) Personal information shall only be transferred to recipients in a Member State that has transposed the SADC data protection requirements –

(a) where the recipient establishes that the data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of a data controller, or

(b) where the recipient establishes the necessity of having the data transferred and there is no reason to assume

that the data subject's legitimate interests might be prejudiced by the transfer or the processing in the Member State.

(2) The controller shall, notwithstanding subsection (1), be required to make a provisional evaluation of the necessity for the transfer of the data.

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

(4) The data controller shall ensure that the recipient shall process the personal information only for the purposes for which they were transferred.

Transfer of personal information to non-SADC Member States

33. (1) Personal information shall only be transferred to recipients, other than in Member States of SADAC, or which are not subject to national law adopted pursuant to SADAC data protection requirements, if an adequate level of protection is ensured in the country of the recipient and the data is transferred solely to permit processing otherwise authorised to be undertaken by the controller.

(2) The adequacy of the level of protection afforded by the relevant third country in question shall be assessed in the light of all the circumstances surrounding the relevant data transfer(s), particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing, the country of the recipient, the relevant laws in force in the third country and the professional rules and security measures which are complied with in that country of the recipient.

(3) The Commission shall establish the categories of processing

for which and the circumstances in which the transfer of personal information to countries outside –

(a) the Kingdom of Eswatini; and

(b) SADC,

is not authorized.

(4) By way of derogation from subsection (3) above, a transfer or a set of transfers of personal information to a recipient in a country outside Eswatini or SADC which does not ensure an adequate level of protection may take place in one of the following cases -

(a) the data subject has unambiguously given their 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 request of the data subject;

(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 defence of legal claims;

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

(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.

(5) Without prejudice to the provisions of the previous paragraph, the Commission may authorize a transfer or a set of transfers of personal information to a recipient country outside Eswatini or SADC which does not in its laws ensure an adequate level of protection, if the controller satisfies the Commission that it shall ensure adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of the data subjects concerned, and regarding the exercise of the rights of the data subject such safeguards can be appropriated through adequate legal and security measures and contractual clauses in particular.

PART VI
ENFORCEMENT

Complaints

34. A person may submit a complaint to the Commission in the prescribed manner and form –

(a) alleging contravention of this Act; or

(b) where the data subject is aggrieved by a determination in terms of an approved code.

Investigation by the Commission

35. (1) The Commission, after receipt of a complaint made in terms of section 34, shall –

(a) investigate any alleged contravention in the prescribed manner;

(b) decide in accordance with Section 36 to take no action on the complaint;

(c) act where appropriate, as conciliator in relation to any such contravention in the prescribed manner, where it appears that it might be possible to secure a settlement between the parties; and

(d) take such further action as is contemplated under this Part.

(2) The Commission may, on its own initiative commence an investigation under subsection (1).

(3) The Commission shall, within a prescribed period advice the complainant and the data controller to whom the complaint relates of the course of action that the Commission shall take.

Reasons for Commission not to take action

36. (1) The Commission may, after receiving a complaint in terms of Section 34, decide not to take any action if, in the opinion of the Commission –

(a) the length of time that has elapsed between the date on which the subject matter of the complaint arose and the date on which the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

(b) the subject matter of the complaint is trivial;

(c) the complaint is frivolous, vexatious or is not made in

good faith;

(d) the complainant does not desire that action be taken or continued;

(e) the complainant does not have sufficient personal interest in the subject matter of the complaint;

(f) the complaint relates to a matter governed by an approved code of conduct which makes provision for a complaints procedure, and the complainant has failed to use the complaints procedure as provided for in that code; or

(g) the complaint relates in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body.

(2) Notwithstanding anything in subsection (1), the Commission may in its discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Commission that any further action is unnecessary or inappropriate.

(3) In any case where the Commission decides to take no action or no further action, on a complaint, the Commission shall inform the complainant of that decision and the reasons for it.

Pre-investigation by the Commission

37. Before proceeding to investigate any matter in terms of this Part, the Commission shall inform the complainant and the data controller to whom the investigation relates of the –

(a) details of the subject matter of the investigation; and

(b) rights of the data controller to submit to the Commission within

fourteen (14) days, a written response in relation to the subject matter of the investigation.

Investigation proceedings by the Commission

38. For the purpose of the investigation of a complaint, the Commission may –

(a) summon and enforce the appearance of persons before the Commission, and compel them to give oral or written evidence under oath and to produce any records and things that the Commission considers necessary to enable it to investigate the complaint;

(b) administer oaths;

(c) receive and accept any evidence and other information whether on oath, by affidavit or otherwise, that the Commission deems fit, whether or not it is or would be admissible in a Court of law;

(d) at any time enter any premises or other place which the Commission reasonably suspects as being connected with any activities regulated by the Commission and search and inspect those premises or other place together with any books, documents or records found on those premises;

(e) require any person to produce for inspection and take extracts from any books, documents, or records relating to any activities regulated by the Commission which are under the control of that person and, in the case of information in a non-legible form or unknown language or encrypted to reproduce that information in a legible form or known language or decrypted, as the case may be, and to give the Commission all the

information requested in relation to any entries in those books, documents or records;

(f) remove and retain the books, documents or records referred to in paragraphs (d) and (e) for such period as may be reasonable for further examination; or

(g) require any person to maintain the books, documents or records referred to in paragraphs (d) and (e) for such period, as may be reasonable as the Commission directs.

Matters exempt from search and seizure

39. (1) Where the Commission has authorised the processing of personal information, the information shall not be subject to search and seizure.

(2) Privileged information shall be exempt from search and seizure.

Parties to be informed of developments and results of an investigation

40. Where the Commission undertakes an investigation following a complaint, and –

(a) the Commission finds that no contravention of this Act has taken place;

(b) the Commission finds that a contravention has taken place;

(c) an enforcement notice is served in terms of section 41;

(d) a served enforcement notice is cancelled in terms of section 42;

(e) an appeal is lodged against the enforcement notice for cancellation or variation of the notice in terms of section 49; or

(f) an appeal against an enforcement notice is allowed, the notice is submitted or the appeal is dismissed,

the Commission shall inform the complainant and the data controller in the prescribed manner, of any developments and the results of the investigation within the prescribed period.

Enforcement notice

41. (1) Where the Commission is satisfied that a data controller has contravened this Act, the Commission shall serve the data controller with an enforcement notice requiring the data controller to do either or both of the following –

(a) to take specified steps within a period specified in the notice, or to refrain from taking action; or

(b) to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice.

(2) An enforcement notice shall include –

(a) a statement indicating the nature of the contravention;

(b) the sanction or decision of the Commission; and

(c) the right to appeal.

Cancellation of enforcement notice

42. (1) A data controller on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal may be brought against that notice, apply in writing to the Commission for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances all or any of the provisions of that notice need not be complied with, in order to ensure compliance with

this Act.

(2) If the Commission considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with this Act, it may cancel or vary the notice by written notice to the party on whom it is served.

Civil remedies

43. A data subject may institute a civil action for damages in a Court having jurisdiction against a data controller for breach of any provision of this Act.

PART VII
GENERAL PROVISIONS

Unsolicited electronic communications

44 (1) In this section “direct marketing” means communication by whatever means of any advertising or marketing material which is directed to particular data subjects.

(2) A data subject is entitled at any time to require a data controller by notice, that the data controller cease, or not begin processing of personal data in respect of which the data subject is the data subject for the purposes of direct marketing.

(3) If the Commission is satisfied on the application of any person who has given notice under subsection (2) that the data controller has failed to comply with the notice, the Commission may order the data controller to take such steps for complying with the notice as the Commission deems fit.

(4) The Commission may regulate issues of unsolicited electronic communications as and when it deems fit in the interests of data subjects.

Automated decision making

45. (1) Subject to subsection (2), a person may not be subjected to a decision which has legal effect on him, or which affects him significantly, based solely on the automated processing of personal information intended to provide a profile of certain aspects of his personality or personal habits.

(2) The provisions of subsection (1) shall not apply where the decision –

(a) has been taken in connection with the conclusion or performance of a contract, and

(i) the request of the data subject in terms of the data contract has been met; or

(ii) appropriate measures have been taken to protect the data subject's legitimate interests such as requiring a data controller to provide a data subject with sufficient information about the decision to enable him to make representations and allowing a data subject to make representations about a decision referred to in subsection (1); or

(b) is governed by a law or code in which appropriate measures are specified for protecting the legitimate interests of data subjects.

(c) is governed by a body of science or scientific proofs or facts with the same measures as in (b).

Notifications

46. (1) A data controller shall notify the Commission of the processing of personal information to which the Act applies.

(2) The notification contemplated in section (1) shall contain the following particulars –

(a) the name and address of the data controller;

(b) the purpose of the processing;

(c) a description of the categories of data subjects and of the information or categories of information relating thereto;

(d) the recipients or categories of recipients to whom the personal information may be supplied;

(e) planned trans-border flow of personal information; and

(f) a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the data controller to ensure the confidentiality, integrity and availability of the information which is to be processed.

(3) Subject to subsection (4), a data controller shall give notice each time personal information is received or processed.

(4) Changes in the name and address of the data controller shall be notified within one (1) week, and changes to the notification which concern subsection (2)(b) to (f) shall be notified within one (1) year of the previous notification, if they are of more than incidental importance.

(5) Any processing which departs from that which has been notified in accordance with the provisions of subsection (2)(b) to (2)(f) shall be recorded and kept for at least three (3) years.

(6) The Commission may –

(a) prescribe more detailed rules concerning the procedure for submitting notifications; and

(b) by notice exempt certain categories of information processing which are unlikely to infringe the legitimate interests of a data subject from the notification requirements referred to in this section.

(7) The Commission shall maintain an up-to-date register of the information processing notified to it.

(8) A data controller shall process personal information only upon notification to the Commission.

Codes of conduct

47. (1) The Commission may, from time to time issue, approve, amend or revoke a code of conduct.

(2) A code of conduct shall incorporate measures that give effect to all information protection principles, given the particular features of the sector or sectors of society in which the relevant data controller is operating.

(3) A code of conduct may apply in relation to any one or more of the following –

(a) specified information or class of information; or

(b) specified body or class of bodies;

(4) The Commission shall ascertain, among other things whether the draft code of conduct submitted to it is in accordance with this law. If it sees fit, the Commission shall seek the views of data subjects or their representatives.

PART VIII

MISCELLANEOUS

Appointment of Data Protection Officers

48. (1) The head of a data controller may, subject to this Act, by order designate one or more officers or employees to be Data Protection Officers of that controller to exercise, discharge or perform any of the power, duties or functions of the head of the data controller under this Act.

(2) An information protection officer's responsibilities shall include, without limitation –

(a) promoting compliance by the controller, with controller's obligations under this Act;

(b) dealing with requests made to the controller pursuant to the controller's obligations under this Act;

(c) cooperating with the Commission in relation to investigations or proceedings conducted in relation to the controller; and

(d) pursuing legal appeals with relevant judicial authorities.

Appeals

49. (1) Subject to the exhaustion of the appeal offered through the Commission under this Act, a data subject shall be entitled to pursue legal appeals with the relevant judicial authorities.

(2) A data controller on whom an enforcement notice has been served, may, within thirty (30) days of receiving the notice apply to a Court having competent jurisdiction for the setting aside or variation of the notice.

(3) A complainant, who has been informed of the result of the investigation may, within thirty (30) days of receiving the result appeal to the High Court against the result of the investigation.

Class actions

50. The Commission shall set up a class action system to assist the data subjects in the exercise of their rights set up under this law.

Whistleblowing

51. (1) The Commission shall establish rules regulating whistleblowing, giving the authorization for, and governing the whistleblowing system.

(2) These rules shall preserve –

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

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

(c) the principle of openness with delivering an adequate collective and individual information on –

(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,

to rectification, deletion as well as the competent authority to which a request can be made;

(v) 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.

(2) A person who is implicated shall be informed as soon as possible of the existence of the reporting and about the facts which that person is accused of in order to exercise the rights under this law including -

(a) the technical and organizational rules;

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

(c) the rules of notification to the Commission.

Other sanctions

52. (1) The Commission may impose a warning to a data controller failing to comply with the obligations of this law, and such warning shall be regarded as a sanction.

(2) In case of serious and immediate violation of the individual rights and liberties, the Commission may rule in summary proceedings –

(a) the limitation or ceasing of the personal data processing;

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

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

(3) A data controller on whom an enforcement notice has been served, may, within thirty (30) days of receiving the notice apply to a Court having competent jurisdiction for the setting aside or variation of the notice.

(4) A complainant, who has been informed of the result of the investigation may, within thirty (30) days of receiving the result appeal to the High Court against the result of the investigation.

Offences and penalties

53. A person who –

(a) hinders, obstructs or unlawfully influences the Commission or any person acting on behalf of or under the direction of the Commission in the performance of the Commission's duties and functions under this Act;

(b) breaches rules of confidentiality made under this Act;

(c) intentionally and unlawfully obstructs a person in the execution of a warrant issued under this Act;

(d) fails, without reasonable cause to give a person executing a warrant assistance as the person may reasonably require for the execution of the warrant; or

(e) violates, without reasonable cause, its obligations under this Act, subject to the determination of the Commission,

commits an offence and shall on conviction be liable to a fine not exceeding One Hundred Million (E100,000,000) Emalangeni or 5 percentage (%) of the annual turnover of the data controller or to imprisonment for a period not exceeding ten (10) years or to both, and if the offender is a

juristic person the sentence shall be served by the head of the data controller.

Regulations

54. (1) The Minister may make regulations generally for the purpose of giving effect to this Act.

(2) The Commission may, as may be necessary for giving effect to this Act, recommend the making of regulations to the Minister.

Transitional provisions

55. (1) Any person, who at the commencement date of this Act is processing any personal information shall, within two (2) years of commencement of this Act bring such processing into conformity with this Act and notify the Commission in terms of this Act.

(2) The period of two (2) years referred to in subsection (1) may be extended to a maximum of three (3) years by the Minister by notice published in the Gazette

---