DATA PROTECTION ACT, 2018

No. 32 **of 2018**

ARRANGEMENT OF SECTIONS

SECTION

PART I — *Preliminary*

1. Short title and commencement
2. Interpretation
3. Application

PART II — *Information and Data Protection Commission*

4. Establishment of Information and Data Protection Commission
5. Functions and powers of Commission
6. Staff of Commission
7. Powers of Commissioner
8. Oath of secrecy
9. Direction by Minister

PART III — *Information and Data Protection Commission's Specific Powers in Relation to Processing of Personal Data*

10. Right of access to information by Commissioner
11. Commission to seek rectification
12. Order to delete personal data
13. Collaboration with other bodies

PART IV — *Requirements and Criteria for Processing Data*

14. Requirements for processing
15. Limitation to processing
16. Criteria for processing
17. Processing for other purposes
18. Processing for direct marketing
19. Revocation of consent

PART V — *Processing of Sensitive Personal Data*

20. Prohibition for processing of sensitive personal data
21. Safeguards for processing sensitive personal data
22. Processing by bodies or entities
23. Processing for health or medical purposes

24. Processing for research, scientific and statistics purposes
25. Processing of genetic and biometric data
26. Processing for legal purposes or by Government
27. Processing of identity card

PART VI — *Data Collection, Right to Access and Duties of Data Controller*

28. Information for data subject
29. Data collected from other sources
30. Rights of data subject
31. Authorisation to process
32. Safeguards for processing of personal data
33. Notification of breach to safeguards
34. Obligation to notify Commissioner
35. Exemption from notification
36. Data protection representative
37. Register maintained by data protection representative
38. Mandatory notification
39. Register maintained by Commissioner
40. Information provided by data controller or data protection representative

PART VII — *Investigations and Enforcement*

41. Investigation by Commissioner
42. Complaints
43. Enforcement notice
44. Variation or revocation of enforcement notice
45. Appeals Tribunal
46. Appeals
47. Proceedings of Tribunal

PART VIII — *Miscellaneous Provisions*

48. Transborder flow of personal data
49. Transfer of personal data to third country
50. Protection from personal liability
51. Offences and penalties
52. Compensation for damages
53. Regulations
54. Transitional provisions

An Act to regulate the protection of personal data and to ensure that the privacy of individuals in relation to their personal data is maintained; to establish the Information and Data Protection Commission; and to provide for all matters incidental thereto.

Date of Assent: 03.08.2018
Date of Commencement: ON NOTICE
ENACTED by the Parliament of Botswana.

PART I — *Preliminary*

Short title and commencement

1. This Act may be cited as the Data Protection Act, 2018 and shall come into operation on such a date as the Minister may, by Order published in the *Gazette*, appoint.

Interpretation

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

"biometric data" means any information stemming from the statistical analysis of biological data;

"block" in relation to personal data, means the operation to suspend modification of data or suspend or restrict the provision of information to a third party when such provision is suspended or restricted in accordance with this Act;

"Commission" means the Information and Data Protection Commission established under section 4;

"Commissioner" means the Commissioner of the Information and Data Protection Commission appointed under section 6;

"consent" means any freely given, specific and informed expression of the wishes of the data subject, by which the data subject agrees to the processing of personal data relating to him or her;

"data controller" means a person who alone or jointly with others, determines the purposes and means of which personal data is to be processed, regardless of whether or not such data is processed by such person or agent on that person's behalf;

"data processor" means a person who processes data on behalf of the data controller;

"data protection representative" means a person who is appointed by the data controller, which person shall independently ensure that personal data is processed in a correct and lawful manner;

"data subject" means an individual who is the subject of personal data;

"direct marketing" means directly reaching a market, customers or potential customers on a personal basis or mass media basis, and it includes attempting to locate, contact, offer and make incentives to consumers, through communication medium such as phone calls, private meetings infomercials, magazines or advertisements;

"file" means any structured set of personal data which is accessible according to specific criteria, whether centralised or dispersed on a functional or geographical basis, regardless of its format or media;

"filing system" means a structured set of personal data which is accessible according to specific criteria, whether centralised, decentralised or disposed on a functional or geographical basis;

"genetic data" personal data relating to the inherited or acquired characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

"identity card number" means the number that appears in the National Identity Card issued in accordance with the National Registration Act; Cap. 01:02

"personal data" means information relating to an identified or identifiable individual, which individual can be identified directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to the individual's physical, physiological, mental, economic, cultural or social identity; and "data" shall be construed accordingly;

"processing of personal data" means any operation or a set of operations which is taken in regard to personal data, whether or not it occurs by automatic means, and includes the collection, recording, organisation, storage, adaptation, alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction of such data; and "processing" shall be construed accordingly;

"recipient" means a person to whom personal data is provided, but does not include —

(*a*) a person who received data in the framework of a particular legal proceeding; and

(*b*) the Commissioner, when the personal data is provided in order to perform the duty to supervise, control or audit;

"sensitive personal data" means personal data relating to a data subject which reveals his or her —

(*a*) racial or ethnic origin;

(*b*) political opinions;

(*c*) religious beliefs or philosophical beliefs;

(*d*) membership of a trade union;

(*e*) physical or mental health or condition;

(*f*) sexual life;

(*g*) filiation; or

(*h*) personal financial information,

and includes —

(*a*) any commission or alleged commission by him or her of any offence;

(*b*) any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings, or the sentence of any court in such proceedings; and

(*c*) genetic data, biometric data and the personal data of minors;

"third country" means a State that is not included in the Order made under section 48;

"third party" means a person other than the data subject, the data controller, the data processor, the data protection representative and such other person authorised by the data controller or data processor;

"transborder flow" means the international flow of personal data which can either be transmitted by electronic or other forms of transmission, including satellite; and

"Tribunal" means the Information and Data Protection Appeals Tribunal established under section 45.

Application

3. (1) This Act shall apply to the processing of personal data entered in a file by or for a data controller —

(*a*) in Botswana; or

(*b*) where the data controller is not in Botswana, by using automated or non-automated means situated in Botswana, unless those means are used only to transmit personal data:

Provided that when the recorded personal data is processed by non-automated means, it forms part of a filing system or is intended to form part of a filing system.

(2) This Act shall not apply to the processing of personal data —

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

(*b*) by or on behalf of the State where the processing —

(i) involves national security, defence or public safety,

(ii) is for the prevention, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures,

(iii) is for economic or financial interest, including monetary, budgetary and taxation matters, and

(iv) is for a monitoring, inspection or regulatory function connected with the exercise of functions under subparagraphs (i), (ii) and (iii).

(3) This Act is exempt from application to the processing of personal data specified under subsection (2) (*b*), to the extent that adequate security safeguards have been established in specific legislation for the protection of such personal data.

PART II — *Information and Data Protection Commission*

Establishment of Information and Data Protection Commission

4. (1) There is hereby established a body to be known as the Information and Data Protection Commission.

Cap. 26:01

(2) The Commission shall be a public office, and the provisions of the Public Service Act shall apply to the Commission and its officers.

Functions and powers of Commission

5. (1) The Commission shall do all such things as are necessary to protect the personal rights of individuals with regard to their personal data, and shall ensure the effective application of and compliance with this Act, in particular, to the right to protection of personal data, access, rectification, objection and cancellation of such data.

(2) Without derogating from the generality of subsection (1), the Commission shall —

Cap. 17:01

(*a*) ensure compliance with the provisions of the Statistics Act —

(i) with regard to the collection of statistical data and statistical secrecy, and

(ii) to issue precise instructions and give opinions on the security safeguards in place, for files set up for purely statistical purposes;

(*b*) instruct a data controller to take such measures which are necessary to ensure that the processing of personal data is in accordance with this Act;

(*c*) provide guidance and instructions on appropriate measures to ensure the security of personal data;

(*d*) conduct research and studies, and promote educational activities relating to protection of personal data;

(*e*) provide information to persons on their rights connected to the processing of personal data;

(*f*) receive reports and claims from a data subject or his or her representative in regard to a violation of this Act, and to take such remedial action as is necessary or as may be prescribed;

(*g*) investigate complaints from data subjects and respond to queries of such complaints;

(*h*) monitor and adopt any authorisation for transborder flow of personal data, and to facilitate international cooperation on the protection of personal data;

(*i*) create and maintain a public register of all data controllers;

(*j*) obtain information from data controllers, which information is necessary for the exercise of its functions;

(*k*) prepare and disseminate a code of practice for data controllers;

(*l*) issue, where applicable, instructions required to bring processing operations in line with the principles of this Act;

(*m*) publicise the existence of personal data files, and regularly publish a list of such files, and any other information that the Commission deems necessary;

(*n*) record all directions received from the Minister in the course of the year; and

(*o*) perform any other functions that may be conferred on it by the Minister.

Staff of Commission

6. (1) The Commission shall consist of a Commissioner, Deputy Commissioner and such other officers as may be necessary for the proper functioning of the Commission.

(2) The Minister shall appoint the Commissioner and the Deputy Commissioner, and the Commissioner shall appoint other officers of the Commission.

(3) The Commissioner shall be responsible for the direction and administration of the Commission.

Powers of Commissioner

7. The Commissioner may, in the performance of the functions of the Commission —

(*a*) authorise any officer of the Commission to conduct an investigation of any alleged breach of the provisions of this Act;

(*b*) require any person, at any specific time, to provide any information required in the process of an investigation conducted under this Act;

(*c*) order or direct an officer of the Commission to block, erase or distribute personal data, whichever is applicable; or

(*d*) do all such things as are necessary to protect the personal rights of individuals with regard to their personal data.

Oath of secrecy

8. The Commissioner and any officer and employee of the Commission shall, before assuming their duties, take an oath of secrecy before the Minister in such form as may be prescribed, to carry out their duties with equity and impartiality and in accordance with the provisions of this Act.

Direction by Minister

9. The Minister may give the Commission directions of a general or specific nature regarding the exercise of its powers and the performance of its functions, which directions shall not be inconsistent with this Act or with the obligations of the Commission, and the Commission shall give effect to any such direction.

PART III — *Information and Data Protection Commission's Specific Powers in Relation to Processing of Personal Data*

Right of access to information by Commissioner

10. (1) The Commissioner shall be entitled to obtain from the data controller, on request made in writing —

(*a*) access to personal data that is processed; and

(*b*) any information or documentation relating to the processing of personal data, and security safeguards of such processing:

Provided that where the personal data is processed for the purpose of compliance with a legal obligation to which the data controller is subject, the Minister may prescribe procedures for purposes of the implementation of paragraph (*a*).

(2) The Commissioner shall at the time of the request made under subsection (1), specify the time in which a data controller shall respond to that request.

(3) Without prejudice to any written law, any person who does not comply with the request made by the Commissioner under subsection (1), or the time specified to respond to such request under subsection (2), commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding three years, or to both.

(4) Where the Commissioner has made a request under subsection (1), and obtains sufficient information in order to conclude that the processing of personal data is unlawful, the Commissioner may prohibit the data controller from processing personal data in any other manner than by storing that data.

(5) In the exercise of the functions of the Commission under this section, the Commissioner may appoint officers for the purposes of inspection, and such officers shall have the same powers to enter and search any premises as are vested in a police officer.

(6) An officer appointed under subsection (5) shall produce an identification card, issued by the Commissioner, to an owner or occupier of any premises.

Commissioner to seek rectification

11. (1) Where the Commissioner concludes, as a consequence of information received in terms of section 10, that the personal data that is processed is incomplete or incorrect, the Commissioner shall order the data controller to complete or correct the processing of such data.

(2) If the personal data is not completed or corrected in terms of subsection (1), or if the matter is urgent, the Commissioner may prohibit the data controller to continue processing the personal data in any other manner than by storing that data.

Order to delete personal data

12. (1) Where the Commissioner decides that personal data has been unlawfully processed, the Commissioner shall, by notice made in writing, order the data controller to delete the personal data.

(2) If the data controller is aggrieved by the decision of the Commissioner, the data controller may, within 30 days of receipt of the notice referred to under subsection (1), appeal against such decision to the Appeals Tribunal.

Collaboration with other bodies

13. The Commission shall, before taking a decision to exercise its functions under section 5 (2) (*b*) and (*k*), which may significantly impact on the operation of any Government Department or of any public or private body, consult a third party who may be directly affected by the decision and the Commission shall give reasons for the decision made.

PART IV — *Requirements and Criteria for Processing Data*

Requirements for processing

14. A data controller shall ensure that —

(*a*) personal data is processed fairly and lawfully, and where appropriate, the data is obtained with the knowledge or consent of the data subject;

(*b*) personal data that is collected is adequate and relevant in relation to the purposes of its processing;

(*c*) to the extent necessary for processing, personal data is accurate, complete and kept up-to-date;

(*d*) personal data is collected for specific, explicitly stated and legitimate purposes;

(*e*) personal data is not processed for any purpose that is incompatible with the specified, explicitly stated and legitimate purposes;

(*f*) personal data is protected by reasonable security safeguards against risks such as loss, unauthorised access, destruction, use, modification or disclosure;

(*g*) where data is incomplete or incorrect, all reasonable measures are taken to complete, correct, block or delete the personal data, having regard to the purposes for which it is processed;

(*h*) personal data is not kept for a period longer than is necessary, having regard to the purposes for which it is processed; and

(*i*) personal data is processed in accordance with good practice.

Limitation to processing

15. Personal data shall not be disclosed, made available or otherwise used for purposes other than those specified, except —

(*a*) with the consent of the data subject; or

(*b*) as may be authorised by any written law.

Criteria for processing

16. Personal data may be processed where —

(*a*) the data subject has given his or her consent in writing;

(*b*) processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;

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

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

(*e*) processing is necessary for the performance of an activity that is carried out in the public interest or in the exercise of an official authorisation vested in the data controller or in a third party to whom the data is disclosed; or

(*f*) processing is necessary for a purpose that concerns a legitimate interest of the data controller, or of a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy.

Processing for other purposes

17. (1) Notwithstanding section 14, personal data may be processed for historical, statistical or scientific purposes.

(2) The data controller shall, when processing data in accordance with subsection (1), ensure that —

(*a*) there are appropriate security safeguards in place where personal data processed for historical, statistical or scientific purposes may be kept for a period longer than is necessary, having regard to the purposes for which it is processed; or

(*b*) personal data kept for historical, statistical or scientific purposes is not used for any decision concerning the data subject.

Processing for direct marketing

18. (1) Subject to subsection (2), where personal data is processed for purposes of direct marketing, the data controller shall, at no cost, inform the data subject of his or her right to oppose the processing.

(2) Where the data subject gives a notice of objection to the processing of his or her personal data for direct marketing, the personal data of the data subject shall not be processed for such purpose.

(3) A data controller who processes data despite the objection of the data subject under subsection (2), commits an offence and is liable to a fine not exceeding P500 000 or to imprisonment for a term not exceeding nine years, or to both.

Revocation of consent

19. (1) Where the processing of personal data takes place with the consent of the data subject, the data subject may at any time, in writing, revoke his or her consent for legitimate grounds compelling him or her at that particular time.

(2) The grounds referred to under subsection (1) shall be legitimate, reasonable and compelling.

PART V — *Processing of Sensitive Personal Data*

Prohibition for processing of sensitive personal data

20. Subject to the provisions of this Part, a person shall not process sensitive personal data, except where —

(*a*) the processing is specifically provided for under this data Act;

(*b*) the data subject has given his or her consent in writing;

(*c*) the data subject has made the data public;

(*d*) the processing is —

(i) necessary for national security,

(ii) necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment, or

(iii) authorised by any other written law, for any reason of substantial interest to the public; or

(*e*) the processing is necessary to protect the vital interest of a data subject or another person in a case where —

(i) consent cannot be given by or on behalf of the data subject,

(ii) the data controller cannot be reasonably expected to obtain consent of the data subject, or

(iii) consent by or on behalf of the data subject has been unreasonably withheld.

Safeguards for processing sensitive personal data

21. A data controller, shall where sensitive personal data is processed, ensure that appropriate security safeguards are adopted.

Processing by bodies or entities

22. (1) A body of persons or an entity, not being a commercial body or entity, which has political, philosophical, religious or trade union objects may, in the course of its legitimate activities and with appropriate guarantees, process sensitive personal data relating to the political, philosophical, religious or trade union objects, whichever is applicable, concerning —

(*a*) the members of that body or entity; or

(*b*) any other person who by reason of the objects of the body or entity, the body or entity regularly exchanges information with.

(2) The sensitive personal data processed under subsection (1) may be provided to a third party only on the written consent of the data subject.

Processing for health or medical purposes

23. (1) A health professional or other person who is subject to the obligation of professional secrecy, may process sensitive personal data for health or medical purposes, where the processing is necessary for —

(*a*) preventive medicine and the protection of public health;

(*b*) medical diagnosis;

(*c*) health care; or

(*d*) the management of health and hospital care services.

(2) For the purposes of this section, a "health professional" means a person registered under the Botswana Health Professions Act, the Nurses and Midwives Act, or any other person under the personal direction or supervision of the health professional and person who is directly authorised to perform such functions.

Cap. 61:02
Cap. 61:03

Processing for research, scientific and statistics purposes

24. (1) Sensitive personal data may be processed for research, scientific and statistics purposes:

Provided that the processing is compatible with specified, explicitly stated and legitimate purposes.

(2) To determine whether the processing of sensitive personal data is necessary under subsection (1), the following shall be satisfied —

(*a*) in the case of research and scientific purposes, that the Commissioner has approved the processing on the advice of a committee responsible for research and scientific ethics in an institution recognised by the Commissioner; and

(*b*) in the case of statistics, the processing is necessary for the purposes provided under the Statistics Act.

Processing of genetic and biometric data

25. (1) The processing of genetic data and biometric data, if it is processed for what it reveals or contains, is prohibited, except where the processing is in accordance with section 20.

(2) Where genetic data and biometric data is processed for medicinal purposes and the consent of the data subject has been granted, such data shall be processed, only if, a unique patient identification number is given to the data subject, which patient identification number is different from any other identification number possessed by the data subject.

Processing for legal purposes or by Government

26. (1) Sensitive personal data may be processed for legal purposes, where it is necessary —

(*a*) in connection with any legal proceedings, including prospective legal proceedings;

(*b*) for the purpose of obtaining legal advice;

(*c*) for the purposes of establishing, exercising or defending legal rights; or

(*d*) for the administration of justice.

(2) Sensitive personal data may be processed by the National Assembly, any Government Department or Ministry, if it is necessary —

(*a*) for the exercise of any function of the National Assembly; or

(*b*) for the exercise of any function of the Government Department or Ministry,

and such processing is compatible with specified, explicitly stated and legitimate purposes.

(3) The Minister responsible for constitutional affairs may, by Order published in the *Gazette* —

(*a*) exclude the application of subsection (1) (*d*) and subsection (2) in such cases as may be specified; or

(*b*) specify further conditions that are to be satisfied to enable the processing under subsection (1) (*d*) and subsection (2).

Processing of identity card

27. A data subject's identity card number may, in the absence of the data subject's consent, only be processed where such processing is clearly justifiable, having regard to —

(*a*) the purpose of the processing;

(*b*) the importance of a secure identification; or

(*c*) any valid reason, as may be prescribed.

PART VI — *Data Collection, Right to Access and Duties of Data Controller*

Information for data subject

28. The data controller or data processor shall, where personal data is obtained directly from the data subject, provide the following information to the data subject, except where the data subject already has the information —

(*a*) the identity and habitual residence or principal place of business of the data controller or data processor;

(*b*) the purpose of the processing for which the personal data is intended;

(*c*) the existence of the right to object to the intended processing, if the processing of the personal data is obtained for the purposes of direct marketing;

(*d*) taking into account the specific circumstances the data is processed, any other additional information, if the information is necessary to ensure fair processing for the data subject, which information may include —

(i) the recipient or category of recipients of the data,

(ii) whether the reply to any question made to the data subject is obligatory or voluntary, as well as the possible consequence of failure to reply, and

(iii) the existence of the right to access, rectify, and where applicable, the right to delete the data concerning him or her; or

(*e*) any other information necessary for the specific nature of the processing, to guarantee fair processing in respect of the data subject.

Data collected from other sources

29. (1) Where personal data is not obtained directly from the data subject, the data controller or data processor shall, except where the data subject already has the information, at least provide the information listed in section 28.

(2) The information referred to under subsection (1) shall be provided —

(*a*) at the time of undertaking the recording of personal data; or

(*b*) if a disclosure to a third party is foreseen, not later than the time when the personal data is first disclosed.

(3) The data controller or data processor may not provide the information required under subsection (1) —

(*a*) if any other law provides for the registration or disclosure of any such personal data, and appropriate security safeguards are adopted;

(*b*) if the personal data is required for —

(i) processing for statistical purposes,

(ii) purposes of historical or scientific research, or

(iii) purposes of medical examination of the population, with a view to protect and promote public health; or

(*c*) if the provision of such information will be impossible or would involve a disproportionate effort.

Rights of data subject

30. (1) A data subject shall have the right to —

(*a*) obtain from a data controller or data processor, confirmation of whether or not the data controller or data processor has personal data relating to him or her;

(*b*) receive communication of personal data relating to him or her within a reasonable time, from the time of request, and at a reasonable charge, if any;

(*c*) be given a reason for refusal of a request made under paragraph (*a*) or (*b*);

(*d*) challenge the refusal for requests made under paragraphs (*a*) and (*b*) and submit a complaint in accordance with section 42 (1); and

(*e*) challenge personal data relating to him or her by submitting a complaint in accordance with section 42 (1), and if the challenge is successful, have the personal data deleted, rectified, completed or amended, whichever is required:

Provided that where the data subject is for any reason unable to challenge personal data relating to him or her then his or her next of kin may submit a complaint on his or her behalf.

(2) Subsection (1) (*a*) and (*b*) shall not apply when the personal data is processed solely for the purpose of scientific research or is kept in a personal form for a period which does not exceed the period necessary for the sole purpose of compiling statistics:

Provided that this subsection shall not apply where the personal data is used for taking a measure or decision regarding any particular individual or where there is a risk of breaching the privacy of the data subject.

Authorisation to process

31. (1) A person who has access to personal data and is acting under the authorisation of the data controller or the data processor, which person includes the data processor, shall process personal data only as instructed by the data controller or the data processor, as the case may be, without prejudice to any duty or restriction imposed by law.

(2) A person who contravenes subsection (1), commits an offence and is liable to a fine not exceeding P20 000 or to imprisonment for a term not exceeding one year, or to both.

(3) A person who processes personal data without authorisation under this section, commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding three years, or to both.

Safeguards for processing of personal data

32. (1) A data controller, a data processor or a person acting under authorisation of the data controller or the data processor, shall, in order to safeguard the security of personal data, take appropriate technical and organisational security measures necessary to protect personal data from —

(*a*) negligent or unauthorised destruction;

(*b*) negligent loss; or

(*c*) alteration, unauthorised access and any other unauthorised processing of personal data.

(2) A data controller, a data processor or a person acting under authorisation of the data controller or the data processor, shall when undertaking the measures under subsection (1), ensure an appropriate level of security by taking into account —

(*a*) technological development of processing personal data, and the costs for implementing the security measures; and

(*b*) the nature of the personal data to be protected and the potential risks involved.

(3) Where the data controller or data processor outsources the processing of personal data, the data controller or data processor shall choose a data processor who gives sufficient guarantees regarding the technical and organisational security measures in place for the processing to be done, and shall ensure that the measures are complied with.

(4) The Commissioner may issue appropriate standards relating to information for security safeguards for all categories of processing personal data.

Notification of breach to safeguards

33. (1) The data controller shall, without delay, notify the Commissioner of any breach to the security safeguards of personal data.

(2) The data processor shall, without delay, notify the data controller of any breach to the security safeguards of personal data, which the data processor holds on behalf of the data controller.

(3) A person who contravenes this section commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding three years, or to both.

Obligation to notify Commissioner

34. (1) The data controller shall notify the Commissioner before carrying out any wholly or partially automated processing operation or set of such operations which are intended to serve a single purpose or several related purposes.

(2) Subsection (1) shall not apply to operations which have the sole purpose of keeping a register that is intended to provide information to the public by virtue of any law, which register is open for public inspection.

(3) The notification under subsection (1) may specify —

(*a*) the name and address of the data controller or data processor;

(*b*) the purpose of the processing;

(*c*) a description of the category or categories of a data subject and of the personal data or categories of personal data relating to the data subject;

(*d*) the recipient or categories of recipients to whom personal data can be disclosed to;

(*d*) proposed transfers of personal data to a third country; and

(*f*) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken under section 32 to ensure security of processing:

Provided that the data controller shall notify the Commissioner of any changes affecting the information referred to under this subsection and the Minister may prescribe any matter related to the form of such notification.

Exemption from notification

35. (1) The Commissioner may exempt a notification required under section 34 (1), where the Commissioner is satisfied that —

(*a*) the personal data being processed has no apparent risk of infringement to the rights of the data subject;

(*b*) the purposes of the processing, the category of processing, the category of a data subject, the category of a recipient, and the data retention period are specified; and

(*c*) the data controller has appointed a data protection representative, and the data controller has notified the Commissioner of such appointment.

(2) Where an exemption is granted under subsection (1), the data controller shall disclose any information required for processing under section 28.

(3) A public body shall not be exempted from notification under section 34 (1), for any processing undertaken by that body.

Data protection representative

36. (1) A data controller may appoint a data protection representative, and shall thereupon notify the Commissioner of such appointment.

(2) A data protection representative appointed under subsection (1) shall —

(*a*) be a person who holds the requisite qualifications; and

(*b*) keep a list of the processing carried out, which list shall be immediately accessible to any person applying for access.

(2) Where a data protection representative is removed, the data controller shall notify the Commissioner of such removal.

(3) Where a data protection representative has been appointed, the notification required under section 34 (1) shall not be required.

(4) A data protection representative shall —

(*a*) ensure that the data controller processes personal data in a lawful and correct manner and in accordance with good practice, and where the data protection representative identifies any inadequacies, he or she shall bring these to the attention of the data controller; and

(*b*) assist the data subject to ensure that his or her rights under the Act are protected.

(5) Where the data protection representative has reason to suspect that the data controller is contravening the rules applicable for processing personal data, and if rectification is not implemented as soon as practicable after such contravention is pointed out, the data protection representative shall notify the Commissioner.

(6) The data protection representative may consult with the Commissioner where there is doubt as to how the rules applicable to processing of personal data are to be applied.

Register maintained by data protection representative

37. (1) A data protection representative shall maintain a register of the processing conducted on behalf of the data controller.

(2) The data protection representative shall, at the instruction of the data controller, provide the information referred to under section 34 (3) (*a*) to (*e*) to any person who requests for it, if that information has not been notified to the Commissioner in terms of section 34.

Mandatory notification

38. (1) An exemption for notification under section 35 (1) shall not apply to processing of personal data that involves a particular risk of improper interference with the rights and freedoms of the data subject, and notification of such processing shall be submitted to the Commissioner, prior to its processing.

(2) The Minister may prescribe the processing operations involving particular risks referred to under subsection (1).

Register maintained by Commissioner

39. The Commissioner shall maintain a register of processing operations notified under section 34 (1), and the register shall contain the information listed under section 34 (3).

Information provided by data controller or data protection representative

40. (1) A data controller or data protection representative, if instructed by the data controller, shall provide to any person who requests for it —

(*a*) any information required under section 34 (3); or

(*b*) any information relating to the processing of personal data that is not notified to the Commissioner under section 34 (3).

(2) This section shall not apply to the information specified under section 34 (2).

PART VII — *Investigations and Enforcement*

Investigation by Commissioner

41. (1) The Commissioner may, either on his or her own initiative or upon receipt of information or a complaint from any person, commence an investigation, where the Commissioner has reasonable grounds to suspect that —

(*a*) there is interference with the protection of personal data;

(*b*) the rights of a data subject are being infringed upon; or

(*c*) personal data is not processed in accordance with this Act.

(2) For the purposes of investigations under this section, any officer of the Commission delegated to investigate may —

(*a*) enter any premises used or apparently used by a data controller, at any reasonable time and search for any record, document or thing that the investigator considers relevant to the investigation;

(*b*) inspect and make copies, or take extracts from, and where necessary in an appropriate case, take possession of such record, document or thing; and

(*c*) direct the data controller or any relevant person, in writing, to —

(i) produce the relevant evidence to the investigator as specified in the direction,

(ii) give the investigator explanations or further information about the relevant evidence, or

(iii) attend before the investigator at a reasonable time and place specified in the direction, and answer under oath, questions relating to the matter.

(3) Section 10 (6) applies to an investigator who enters any premises under this section.

Complaints

42. (1) A person may submit a complaint in writing, to the Commissioner —

(*a*) alleging interference with the protection of personal data; or

(*b*) against a decision made under this Act, of which the data subject or his or her next of kin is aggrieved.

(2) The Commissioner may, where he or she is satisfied that there is a need to investigate a complaint brought under subsection (1), direct an investigation to be conducted in terms of section 41.

Enforcement notice

43. (1) Where the Commissioner is satisfied that any person has interfered or is interfering with the protection of personal data, the Commissioner may serve the person with an enforcement notice, requiring that person —

(*a*) to take such steps as may be specified in the enforcement notice, within the time specified therein; or

(*b*) within a period specified in the notice, to stop —

(i) processing the personal data specified in the notice, or

(ii) processing personal data for the purpose or in a manner specified in the notice.

(2) An enforcement notice referred to under subsection (1) shall contain a statement indicating the nature of the interference with the protection of personal data, and the reasons for the decision to issue the enforcement notice.

Variation or revocation of enforcement notice

44. (1) The Commissioner may vary or revoke an enforcement notice at his or her own instance, or by request made in application by the person issued with the notice.

(2) The Commissioner may vary or revoke an enforcement notice if he or she is satisfied that, due to a change in circumstances, all or any of the provisions of the notice need not be complied with.

(3) An application to vary or revoke an enforcement notice under subsection (1) shall be in such manner and upon payment of such fee as may be prescribed.

Appeals Tribunal

45. (1) There shall be established an Information and Data Protection Appeals Tribunal to adjudicate over matters brought before the Tribunal for breach of any of the provisions of this Act.

(2) The Tribunal established under subsection (1) shall consist of —

(*a*) a Chairperson, who shall be a High Court judge, a retired High Court judge or a legal practitioner who qualifies to be appointed as a High Court judge; and

(*b*) two other persons who, in the opinion of the Minister, represent the interests of data subjects and of data controllers.

(3) The members of the Tribunal shall be appointed by the Minister for a term of three years, and shall be eligible for re-appointment for a further term of three years.

(4) The members of the Tribunal shall be paid such allowances as shall be determined by the Minister.

Appeals

46. (1) A person aggrieved by the decision of the Commissioner to —

(*a*) serve him or her with an enforcement notice; or

(*b*) refuse to vary or revoke an enforcement notice, may, within 30 days of such decision, appeal to the Appeals Tribunal established under section 45.

(2) In determining an appeal under this section the Tribunal may —

(*a*) dismiss the appeal; or

(*b*) reverse, amend or vary the decision of the Commissioner.

Proceedings of Tribunal

47. (1) The Tribunal shall sit as and when it has received a complaint.

(2) The Tribunal may call such witnesses or request the production of such documents as is necessary for the conduct of the proceedings before the Tribunal.

(3) A witness appearing before the Tribunal shall be entitled to the same allowances as those of a witness in proceedings before a magistrates' court.

(4) Subject to the provisions of this Act, the Tribunal may regulate its own procedure.

PART VIII — *Miscellaneous Provisions*

Transborder flow of personal data

48. (1) The transfer of personal data from Botswana to another country is prohibited.

(2) Notwithstanding the generality under subsection (1), the Minister may, by Order published in the *Gazette*, designate the transfer of personal data to any country listed in such Order.

Transfer of personal data to third country

49. (1) Without prejudice to section 48, and subject to the provisions of this Act, the transfer of personal data that is undergoing processing or intended processing, to a third country may only take place if the third country to which the data is transferred ensures an adequate level of protection.

(2) The adequacy of the level of protection of data by a third country referred to under subsection (1) shall be assessed by the Commissioner in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations, and particular consideration shall be given to —

(*a*) the nature of the data;

(*b*) the purpose and duration of the proposed processing operation;

(*c*) the country of origin and country of final destination;

(*d*) the rule of law, both general and sectoral, in force in the third country in question; and

(*e*) the professional rules and security safeguards which are complied with in that country.

(3) The Commissioner shall decide whether a third country ensures adequate security safeguards.

(4) The transfer of personal data to a third country that does not ensure adequate security safeguards is prohibited.

(5) Notwithstanding subsection (4), a transfer of personal data to a third country that does not ensure adequate security safeguards may be effected by the data controller if the data subject has given his or her consent to the proposed transfer or if the transfer —

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

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

(*c*) is necessary or legally required for the public interest, or for the establishment, exercise or defence of a legal claim;

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

(*e*) is made from a register that according to any law, is intended to provide information to the public and which is open for public inspection.

(6) Notwithstanding subsection (1), the Commissioner may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of security safeguards within the meaning of subsection (2):

Provided that the data controller provides adequate safeguards, which may result by means of appropriate contractual provisions, with respect to the protection of the privacy and fundamental rights and freedoms of individuals and with respect to their exercise.

Protection from personal liability

50. No matter or thing done or omitted to be done by the Commissioner or any officer of the Commission shall, if the matter or thing is done or omitted to be done *bona fide* in the course of the operations of the Commission, render the Commissioner or officer or any person acting under the direction of the Commissioner, personally liable to an action, claim or demand.

Offences and penalties

51. (1) A person who processes personal data in contravention of this Act commits an offence and is liable to a fine not exceeding P300 000 or to imprisonment for a term not exceeding seven years, or to both.

(2) A person who processes sensitive personal data in contravention of this Act commits an offence and is liable to a fine not exceeding P500 000 or to imprisonment for a term not exceeding nine years, or to both.

(3) A data controller who processes personal data in contravention of this Act commits an offence and is liable to a fine not exceeding P500 000 or to imprisonment for a term not exceeding nine years, or to both.

(4) A data controller who processes sensitive personal data in contravention of this Act commits an offence and is liable to a fine not exceeding P1 000 000 or to imprisonment for a term not exceeding 12 years, or to both.

(5) A data controller who does not inform a data subject of the rights conferred on the data subject under this Act commits an offence and is liable to a fine not exceeding P100 000 or to imprisonment for a term not exceeding three years, or to both.

(6) Where a data controller does not implement the security safeguards under section 32, the data controller shall be liable to a fine of P500 000 or to imprisonment for a term not exceeding nine years, or to both.

Compensation for damages

52. (1) A data subject may institute an action for damages against a data controller who processes data in contravention of this Act.

(2) An action under this section shall be commenced within a period of 12 months from the date when the data subject became aware or could have become aware of such contravention, whichever is earlier.

Regulations

53. (1) The Minister may make regulations prescribing anything under this Act which is to be prescribed or which is necessary for the better carrying out of the objects and purposes of this Act or to give force and effect to its provisions.

(2) Without derogating from the generality of subsection (1), regulations may provide for —

(*a*) additional criteria for the processing of personal data;

(*b*) procedures for the implementation of access to personal data;

(*c*) processing operations; and

(*d*) a code of practice or rules relating to the processing of data.

Transitional provisions

54. (1) The processing of personal data by any person, which was ongoing before the commencement of this Act or is ongoing and does not conform to the provisions of this Act, shall, within a period of 12 months from the commencement of this Act, be made by such person to conform to the provisions of this Act.

(2) A person who does not comply with subsection (1) commits an offence and is liable to the penalties set out under section 51.

PASSED by the National Assembly this 12th day of July, 2018.

BARBARA N. DITHAPO,
Clerk of the National Assembly.