DATA PROTECTION ACT, 2024

No. 18 **of 2024**

ARRANGEMENT OF SECTIONS

SECTION

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

Date of Assent: 24.10.2024
Date of Commencement: ON NOTICE
ENACTED by the Parliament of Botswana.

PART I — *Preliminary Provisions*

Short title and commencement

1. This Act may be cited as the Data Protection Act, 2024 and shall come into operation on such date as the Minister may, by Order published in the *Gazette*, appoint.

Interpretation

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

"binding corporate rules" means personal data protection policies which are —

(*a*) adhered to by a data controller or data processor established in Botswana or another country for the transfer or a set of transfers of personal data to a data controller or data processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity; and

(*b*) approved by the Commission in terms of section 77;

"biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

"child" has the meaning assigned to under the Children's Act; Cap. 28:04

"Commission" means the Information and Data Protection Commission continued under section 6;

"Commissioner" means the Commissioner of the Information and Data Protection Commission appointed in terms of section 8;

"consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her and given in terms of section 27 or 29;

"data controller" means a person or public authority which, alone or jointly with others, and in accordance with Part X, determines the purposes and means of the processing of personal data;

"data processor" means a person who processes personal data on behalf of the data controller in terms of sections 55 and 56;

"data protection officer" means a person designated as such under section 69;

"data subject" means a natural person who is the subject of personal data;

"Deputy Commissioner" means a Deputy Commissioner appointed in terms of section 8;

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

"genetic data" means personal data relating to the inherited or acquired genetic 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;

"information society services" means any service provided for remuneration, at a distance, by electronic means and at the request of the person receiving such service;

"international organisation" means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;

"personal data" means any information relating to an identified or identifiable natural person, or data subject; and an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, and includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

"pseudonymisation" means processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information:

Provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

"public authority" has the same meaning as assigned to it under the Access to Information Act;

Act No. 16 of 2024

"recipient" means a natural or legal person, or a public authority, to which personal data is disclosed, whether a third party or not;

"representative" means a natural or legal person established in Botswana who, designated by the controller or processor in writing in terms of section 54, represents the controller or the processor with regard to their respective obligations under this Act;

"restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future;

"sensitive personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, and includes personal data relating to a data subject which reveals —

(*a*) commission or any 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 personal data of a minor in terms of section 30; and

"third party" means a natural or legal person, or public authority, other than the data subject, data controller, data processor and persons who, under the direct authority of the data controller or data processor, are authorised to process personal data.

Objects of the Act

3. The objects of this Act are to —

(*a*) lay down the rules relating to the —

(i) protection of natural persons with regard to the processing of personal data, and

(ii) free flow of personal data in the provision of goods and services; and

(*b*) protect fundamental rights and freedoms of natural persons insofar as they relate to privacy and the protection of personal data.

Application

4. (1) This Act shall apply to —

(*a*) automated processing of all or part of personal data by a data controller or data processor established in Botswana; and

(*b*) non-automated processing, by a data controller or data processor established in Botswana, of personal data contained in a file or intended to form part of a filing system.

(2) In the case of a data controller or data processor who is not established in Botswana, this Act shall apply where —

(*a*) the activities of an establishment of the data controller or data processor are in Botswana, irrespective of whether such processing takes place in Botswana; or

(*b*) processing activities relate to the —

(i) offering of goods or services to data subjects in Botswana, irrespective of whether payment by a data subject is required, or

(ii) monitoring of data subjects' behaviour, insofar as the behaviour takes place within Botswana.

(3) This Act shall not apply to 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 persecution 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).

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

Act binds state

5. This Act binds the State.

PART II — *Continuation of Information and Data Protection Commission*

Continuation of Information and Data Protection Commission Cap. 26:01

6. (1) There shall continue to be a body known as the Information and Data Protection Commission.

(2) The Commission shall be a public office, and the provisions of the Public Service Act shall, with such modifications as may be necessary, apply to the Commissioner, Deputy Commissioners and officers of the Commission.

(3) The Commission shall consist of —

(*a*) a Commissioner;

(*b*) such number of Deputy Commissioners as may be necessary for purposes of section 7 (1); and

(*c*) such other officers of the Commission, as may be necessary for the proper performance of the functions of the Commission.

Divisions of Commission

7. (1) There shall be —

(*a*) a Data Protection Division of the Commission which shall be responsible for data protection in the execution of the functions of the Commission under this Act;

(*b*) an Access to Information Division of the Commission which shall be responsible for access to information in the execution of the functions of the Commission under the Access to Information Act; and

(*c*) such other divisions of the Commission as may be necessary for the proper performance of the functions of the Commission under this Act.

(2) Each of the divisions of the Commission under subsection (1) shall be —

(*a*) headed by a Deputy Commissioner, who shall be the administrative head of the division; and

(*b*) subject to the control and directions of the Commissioner, be responsible for the efficient management, administration and control of the division.

Appointment of Commissioner

8. (1) The Commissioner and Deputy Commissioners shall be appointed by the President acting on the advice of the Minister who shall have —

(*a*) the qualifications, experience and skills, in particular in the area of data science, information technology, law or any field related to the protection of personal data and access to information; and

(*b*) eligibility conditions for appointment and re-appointment:

Provided that in advising the President, the Minister shall not recommend a person unless such person holds a Masters degree from a recognised university in any field under paragraph (*a*);

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

(3) A person appointed as Commissioner shall hold office for a five year renewable term or until he or she attains the age of 60 years, whichever is the earlier.

(4) A person holding the office of the Commissioner may be removed from office for —

(*a*) inability to perform the functions of his or her office arising from infirmity of body, mind or any other cause;

(*b*) gross misconduct; or

(*c*) incompetence.

(5) The provisions of section 113 (3), (4) and (5) of the Constitution shall apply with necessary modifications to the removal of a person holding office of Commissioner.

Oath of secrecy

9. The Commissioner, the Deputy Commissioner, every officer and support staff on being appointed to the Commission shall, before assuming the duties of his or her office, make and subscribe to the oaths or affirmations as may be prescribed —

(*a*) in the case of the Commissioner and Deputy Commissioner, before the President; and

(*b*) in the case of any other officer, before the Commissioner.

Operational independence of Commission

10. (1) The Commission shall act with complete operational independence in performing its functions and exercising its powers in accordance with this Act.

(2) The Commissioner, Deputy Commissioner and officers of the Commission shall —

(*a*) in the performance of their duties, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from any person; and

(*b*) refrain from any action incompatible with their duties and shall not, during their term of office, engage in any incompatible occupation, whether gainful or not.

(3) Any decision, including investigations by the Commissioner shall not be subject to the direction and control of any person or authority.

Confidentiality

11. The Commissioner, Deputy Commissioner and any officer of the Commission shall —

(*a*) during their term of office, maintain confidentiality of any confidential information acquired in the discharge of their duties under this Act; and

(*b*) not disclose any information from which an individual can be identified which is acquired by the Commission in the course of carrying out its functions except where such disclosure is necessary —

(i) to enable the Commission to carry out its functions,
(ii) for the prevention or detection of a criminal offence,
(iii) for the discharge of any international obligation to which Botswana is subject, or
(iv) pursuant to an order of court.

(3) A Commissioner, Deputy Commissioner or officer of the Commission who contravenes this section commits an offence and is liable to a fine not exceeding P50 000 or to imprisonment for a term not exceeding three years, or to both.

PART III — *Competence and Powers of the Commission*

Competence of Commission

12. The Commission shall be the national supervisory authority responsible for ensuring effective application of, and compliance with, this Act.

Duties of Commission

13. (1) Without prejudice to section 12, the Commission shall —

(*a*) monitor and enforce the application of this Act;
(*b*) promote public awareness and understanding of the risks, rules, safeguards and rights of data subjects, and in particular the risks, rules and safeguards where the data subject is a child, in relation to processing;
(*c*) pursuant to section 17, advise public authorities and other entities on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing;
(*d*) promote the awareness of data controllers and data processors of their obligations under this Act;
(*e*) upon request, provide information to any data subject concerning the exercise of their rights under this Act;
(*f*) handle complaints lodged by a data subject in accordance with section 80, and investigate, to the extent necessary, the subject matter of the complaint and inform the complainant of the progress and the outcome of the investigation within a reasonable period, as may be prescribed;
(*g*) conduct investigations on the application of this Act;
(*h*) monitor relevant developments, insofar as they have an impact on the protection of personal data, and in particular the development of information and communication technologies and commercial practices;
(*i*) establish and maintain a list of processing operations which are subject to the requirement for a data protection impact assessment in terms of section 66;
(*j*) keep internal records of contraventions of this Act and of measures taken in accordance with section 16; and
(*k*) perform any other duties related to the protection of personal data.

(2) The Commission shall facilitate the submission of complaints under subsection (1) (*f*) in such manner as may be prescribed.

(3) The performance of the duties under this section shall be free of charge for the data subject.

Investigative powers of Commission

14. The Commission shall have powers to —

(*a*) order the data controller and data processor, and where applicable, the data controllers or processors representative to provide any information it requires for the performance of its duties;

(*b*) carry out investigations in the form of data protection audits;

(*c*) notify the data controller or data processor of an alleged contravention of this Act;

(*d*) obtain, from the data controller and the data processor, access to all personal data and to all information necessary for the performance of its duties; and

(*e*) obtain access to any premises of the data controller and data processor, including to any data processing equipment and means.

Powers of search, seizure and detention

15. (1) Subject to subsection (2), an officer of the Commission who is duly authorised by the Commissioner may, pursuant to section 14, enter any premises for the purpose of conducting a search and may seize any item during the course of an investigation.

(2) The authorised officer shall not enter, conduct a search or seize any item in terms of subsection (1) unless he or she has obtained —

(*a*) the consent, in writing, of the owner or of the person in charge of the premises; or

(*b*) a search warrant.

(3) The authorised officer shall carry at all times and present an identity card issued by the Commission, as may be prescribed.

(4) Any person who obstructs or interferes with the authorised officer in the performance of his or her functions under this section commits an offence and is liable to a fine not exceeding P500 000 or to imprisonment for a term not exceeding ten years, or to both.

Corrective powers of Commission

16. The Commission shall have powers to —

(*a*) issue a warning to a data controller or data processor that the intended processing operations are likely to contravene the provisions of this Act;

(*b*) issue a reprimand to a data controller or data processor where processing operations contravene the provisions of this Act;

(*c*) order the data controller or the data processor to comply with the data subject's requests to exercise his or her rights pursuant to this Act;

(*d*) order, where appropriate, the data controller or data processor to bring processing operations into compliance with the provisions of this Act in a specified manner and within a specified period;

(*e*) order the data controller to communicate a personal data breach to the data subject;

(*f*) impose a temporary or definitive restriction, including a ban on processing;

(*g*) order the rectification or erasure of personal data or restriction of processing pursuant to sections 43 to 45 and the notification of such actions to recipients to whom the personal data have been disclosed pursuant to section 46;

(*h*) impose an administrative fine pursuant to section 83, in addition to measures under this section; and

(*i*) order the suspension of data flows to a recipient in a third country or to an international organisation.

Authorisation and advisory powers of Commission

17. The Commission shall have powers to —

(*a*) advise the data controller in accordance with the prior consultation procedure under section 68;

(*b*) approve draft codes of conduct pursuant to section 73;

(*c*) develop and issue standard contractual clauses in terms of section 59 and adopt standard data protection clauses in accordance with section 76 (2) (*c*);

(*d*) authorise administrative arrangements under section 76 (3) (*b*); and

(*e*) approve binding corporate rules pursuant to section 77.

Activity reports

18. (1) The Commission shall, within a period of six months after the end of the financial year, or such extended period as the Minister may direct —

(*a*) draw up an annual report on its activities, which may include a list of types of contraventions notified and types of measures taken in accordance with section 16; and

(*b*) submit the annual report to the Minister in such form and manner as may be prescribed.

(2) The Minister shall lay the annual report before the National Assembly within three months of receipt.

PART IV — *Principles Relating to Processing of Personal Data*

Lawfulness, fairness and transparency

19. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation

20. Personal data shall be collected for a specified, explicit and legitimate purpose, and shall not be further processed in a manner that is incompatible with the initial purpose:

Provided that further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with section 35 shall not be considered incompatible with the legitimate purpose.

Data minimisation

21. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

Accuracy

22. (1) Personal data shall be accurate and, where necessary, kept up to date.

(2) Pursuant to subsection (1), a data controller or data processor shall take reasonable steps to ensure that personal data that is inaccurate, having regard to the purpose for which it is processed, is erased or rectified without delay.

Storage limitation

23. (1) A data controller or data processor shall ensure that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed.

(2) Notwithstanding subsection (1), and subject to implementation of the appropriate technical and organisational measures required in section 62 to safeguard the rights and freedoms of the data subject, personal data may be stored for an extended period where such personal data will be processed in terms of section 35 solely for —

(*a*) archiving purposes in the public interest;

(*b*) scientific or historical research purposes; or

(*c*) statistical purposes.

Integrity and confidentiality

24. Personal data shall be processed using the appropriate technical or organisational measures required in section 62 and in a manner that ensures the appropriate security of the personal data, including protection against —

(*a*) unauthorised or unlawful processing; and

(*b*) accidental loss, destruction or damage.

Accountability

25. A data controller shall be responsible for, and be able to demonstrate, compliance with sections 19 to 24.

PART V — *Legal Basis for Processing of Personal Data*

Lawfulness of processing

26. Processing shall be lawful only to the extent that at least one of the following applies —

(*a*) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(*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 or of another natural person;

(*e*) processing is necessary for the performance of a duty carried out in the public interest or in the exercise of an official authority vested in the data controller; or

(*f*) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where —

(i) such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, or

(ii) processing is carried out by a public authority when performing its functions.

Conditions for consent

27. (1) Where processing is based on consent, the data controller shall demonstrate that the data subject has consented to the processing of his or her personal data.

(2) If the data subject's consent is given in the form of a written declaration which also concerns other matters, the request for consent shall be presented —

(*a*) in a manner which is clearly distinguishable from the other matters; and

(*b*) in an intelligible and easily accessible form using clear and plain language.

(3) Any part of a declaration under subsection (2) which contravenes the provisions of this Act shall not be binding.

(4) Where the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract or provision of that service, the consent shall, notwithstanding that it is freely given, be deemed invalid.

Right to withdraw consent

28. (1) The data subject shall have the right to withdraw his or her consent at any time.

(2) The withdrawal of consent pursuant to subsection (1) shall —

(*a*) not affect the lawfulness of processing based on consent before its withdrawal; and

(*b*) be done in like manner, and in all respects, as the same might have been done when giving consent.

(3) Prior to obtaining consent, the data controller shall inform the data subject of his or her right under subsection (1).

Conditions applicable to children in relation to information society services

29. (1) Where processing of personal data of a child relates to the offer of information society services, such processing of personal data shall be lawful only to the extent that consent is given or authorised by a parent or person who has parental duties over the child in terms of the Children's Act:

Provided that where the child is 16 years of age, such child may give consent in such manner as may be prescribed.

(2) For purposes of subsection (1), the data controller shall, where appropriate and taking into account available technology, make reasonable efforts to verify that consent is given jointly by the child and the parent or person who has parental duties over the child.

PART VI — *Processing of Sensitive Personal Data*

Processing of sensitive personal data

30. (1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

(2) Subsection (1) shall not apply if —

(*a*) the data subject has given explicit consent to the processing of his or her personal data for one or more specified purposes, except where the law to which the data controller is subject provides that the prohibition in subsection (1) may not be lifted by the data subject;

(*b*) processing is necessary for purposes of carrying out the obligations and exercising specific rights of the data controller or data subject in employment and social protection insofar as it is authorised by law or a collective agreement, and subject to the appropriate safeguards for fundamental rights and interests of data subject;

(*c*) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(*d*) processing relates to personal data which is manifestly made public by the data subject;

(*e*) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(*f*) processing is necessary for reasons of substantial public interest, on the basis of a law that —

(i) is proportionate to the aim pursued, respects the essence of the right to data protection, and

(ii) provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(*g*) processing is necessary for —

(i) the purposes of preventive or occupational medicine,

(ii) the assessment of the working capacity of an employee,

(iii) medical diagnosis,

(iv) the provision of health or social care or treatment, or

(v) the management of health or social care systems and services;

(*h*) processing is necessary for reason of public interest in the area of public health, including —

(i) protection against serious cross-border threats to health, and

(ii) ensuring high standards of quality and safety of health care and of medicinal products or medical devices; or

(*i*) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or

(*j*) processing is carried out in the course of elections for purposes of compiling data on political opinions by a political party, candidate for election or holder of a political office.

(3) For purposes of —

(*a*) subsection (2) (*h*), personal data in subsection (1) may be processed when such data is processed by or under the responsibility of a professional subject to the obligation of professional secrecy or rules established by a professional body in accordance with the law regulating that profession; and

(*b*) subsection (2) (*i*) and (*j*), personal data shall be processed when such processing is proportionate to the aim pursued, respects the essence of the right to data protection and provide suitable and specific measures to safeguard fundamental rights and interests of the data subject.

Processing of sensitive data by entities

31. (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 or former members of that body;

(*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 of personal data relating to criminal convictions and offences

32. Processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of a public authority, or when the processing is authorised by law, providing for appropriate safeguards for the rights and freedoms of data subjects.

Processing which does not require identification

33. (1) Where the purpose for which a data controller processes personal data does not or no longer requires the identification of a data subject by the data controller, the data controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject.

(2) Where in terms of subsection (1), the data controller is able to demonstrate that it is not in a position to identify the data subject, the data controller shall inform the data subject accordingly, if possible.

(3) Notwithstanding subsection (2), sections 42 to 49 shall not apply except where the data subject for the purpose of exercising his or her rights under those sections, provides additional information enabling his or her identification.

PART VII — *Provisions Relating to Specific Processing Situations*

Processing and public access to official documents

34. In order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Act, personal data in official documents held by a public authority or other entity for the performance of a duty carried out in the public interest may be disclosed by the public authority or other entity in accordance with the law to which the public authority or private body is subject.

Processing for archiving, research or statistical purposes

35. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to the appropriate safeguards for the rights and freedoms of the data subject and technical and organisational measures in order to ensure respect to the principle of data minimisation.

Obligations of secrecy

36. An obligation of professional secrecy or other equivalent obligations of secrecy, where this is necessary and proportionate to reconcile the right of the protection of personal data with the obligation of secrecy, shall apply only with regard to personal data which the data controller or data processor has received as a result of or has obtained in an activity covered by that obligation of secrecy.

PART VIII — *Rights of Data Subjects*

Transparent information and communication

37. (1) Where any information is specifically addressed to a data subject, the data controller shall take appropriate measures to provide information relating to processing in a concise, transparent, intelligible and easily accessible form using clear and plain language.

(2) The information in subsection (1) shall be provided in writing, including where appropriate, by electronic means.

(3) When requested by the data subject, the information may be provided orally:

Provided that the identity of the data subject is proven.

Modalities for exercising rights of data subject

38. (1) The data controller shall facilitate the exercise of data subject rights under sections 42 to 49.

(2) The data controller shall, in relation to section 35, not refuse to act on the request of the data subject, except where the data controller is able to demonstrate under section 33 (1) and (2) that it is not in a position to identify the data subject.

(3) The data controller shall, on request being made by the data subject, provide information on any action taken under sections 42 to 49 to the data subject without undue delay, and in any event within one month of receipt of the request or such lesser period as may be determined by the Commission.

(4) The period in subsection (3) may, taking into account the complexity and number of the requests and with the approval of the Commission, be extended by a period not exceeding two months.

(5) The data controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

(6) Where the data subject makes the request by electronic means, the information shall be provided by electronic means, unless the data subject requests otherwise.

(7) If the data controller does not take action on the request of the data subject, the data controller shall inform the data subject without delay, and at the latest within one month of receipt of the request, of the —

(*a*) reasons for not taking action; and

(*b*) data subject's right to lodge a complaint with the Commission and to seek a judicial remedy.

(8) No charge shall be levied by the data controller for information provided under sections 39 to 41 or any communication and action taken under sections 42 to 49:

Provided that where requests from a data subject are manifestly unfounded or excessive, because of their repetitive character, the data controller may —

(i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or

(ii) refuse to act on the request.

(9) The data controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Information provided when personal data is collected from data subject

39. (1) Where personal data relating to a data subject is collected from the data subject, the data controller shall, at the time when personal data is obtained, provide the data subject with —

(*a*) the identity and contact details of the data controller and where applicable the controller's representative;

(*b*) the contact details of the data protection officer;

(*c*) the purpose of processing for which personal data is intended and the legal basis for processing;

(*d*) where processing is based on section 26 (*f*), the legitimate interests pursued by the data controller or a third party; and

(*e*) the recipients or categories of recipients of the personal data, if any.

(2) In addition to subsection (1), the data controller shall, where applicable, inform the data subject —

(*a*) that the data controller intends to transfer personal data to a third country or international organisation; and

(*b*) of the existence or absence of an adequacy decision in terms of section 75.

(3) In the case of transfers under sections 76, 77 or 78 (1), the data controller shall provide the data subject with —

(*a*) reference to the appropriate or suitable safeguards; and

(*b*) the means by which to obtain a copy, if the safeguards are made available.

Further information to ensure transparent processing

40. (1) In addition to the information under section 39, the data controller shall, at the time when personal data is obtained from the data subject, provide the data subject with the following further information necessary to ensure fair and transparent processing —

(*a*) the period personal data will be stored, or if that is not possible, the criteria that will be used to determine that period;

(*b*) the existence of the right to request from the data controller —

(i) access to, rectification or erasure of personal data under sections 42 to 44, or

(ii) restriction of processing under section 45;

(*c*) the existence of the right to data portability under section 47 and the right to object to processing under section 48;

(*d*) where —

(i) processing is based on consent in terms of section 26 (*a*), or

(ii) the data subject has given explicit consent in terms of section 30 (2) (*a*),

the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(*e*) the right to lodge a complaint with the Commission under section 80;

(*f*) whether, in terms of section 30 (2) (*b*) or (*f*), the provision of personal data is a statutory or contractual requirement, and whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;

(*g*) the existence under section 49 of automated decision-making, including —

(i) profiling and meaningful information about the logic involved, and

(ii) the significance and the envisaged consequences of such processing for the data subject.

(2) Where the data controller intends to further process personal data for a purpose other than that for which the personal data was collected, the data controller shall provide the data subject, prior to that further processing, with information on that other purpose and with any relevant further information in section 41.

(3) Section 39 and this section shall not apply where, and insofar as, the data subject already has the information.

Information provided when personal data is not obtained from data subject

41. (1) Where personal data is not obtained from the data subject, the data controller shall provide the data subject —

(*a*) with the information specified in sections 39 and 40;

(*b*) with the source from which the personal data originates, and if applicable, whether it came from a publicly accessible source; and

(*c*) with the categories of personal data concerned.

(2) The data controller shall provide the information in subsection (1) —

(*a*) within a reasonable period after obtaining the personal data, but not exceeding one month, having regard to the specific circumstances in which the personal data is processed;

(*b*) if the personal data is to be used for communication with the data subject, at the time of the first communication to that data subject; or

(*c*) if a disclosure to another recipient is envisaged, when the personal data is first disclosed.

(3) Where the data controller intends to further process the personal data for a purpose other than the initial purpose, the data controller shall, prior to that further processing, provide the data subject with information on that other purpose and with any relevant further information under section 40.

(4) Subsections (1) to (3) shall not apply where, and insofar as —

(*a*) the data subject already has the information;

(*b*) the provision of such information —

(i) proves impossible or would involve a disproportionate effort in relation to section 35, or

(ii) the obligations under subsections (1) to (3) are likely to render impossible or seriously impair the achievement of the objectives of that processing;

(*c*) obtaining or disclosure is expressly provided by law; or

(*d*) where the personal data remains confidential subject to an obligation of professional secrecy, including a statutory obligation of secrecy pursuant to section 30 (3).

(5) For purposes subsection (4) (*b*), the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.

Right of access by data subject

42. (1) The data subject shall have the right to obtain from the data controller confirmation as to whether personal data concerning him or her is being processed, and, where that is the case, access to the personal data and the information relating to —

(*a*) the purpose of processing;

(*b*) the categories of personal data concerned;

(*c*) the recipient or categories of recipients to whom the personal data has been or will be disclosed, and in particular recipients in third countries or international organisations;

(*d*) the envisaged period for which the personal data will be stored, or if not possible the criteria used to determine the period;

(*e*) the existence of the right to object to processing of personal data or to request from the data controller —

(i) rectification or erasure personal data,

(ii) restriction of processing of personal data;

(*f*) the existence of the right to lodge a complaint;

(*g*) the source of information, where the personal data is not collected from the data subject; and

(*h*) the existence of automated decision-making, including profiling and meaningful information about the logic involved as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data is transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to section 76.

(3) The data controller shall provide a copy of the personal data undergoing processing:

Provided that for any further copies requested by the data subject, the data controller may charge a reasonable fee based on administrative costs.

(4) Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

(5) The right to obtain a copy under subsection (3) shall not adversely affect the rights and freedoms of other persons.

Right to rectification

43. The data subject shall have the right —

(*a*) to obtain from the data controller, without undue delay, the rectification of inaccurate personal data concerning him or her; and

(*b*) taking into account the purpose of processing, to have incomplete personal data completed, including providing a supplementary statement.

Right to erasure

44. (1) The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him or her without undue delay, and the data controller shall have the obligation to erase the personal data without undue delay where one of the following grounds applies —

(*a*) personal data is no longer necessary in relation to the purpose for which it was collected or otherwise processed;

(*b*) the data subject withdraws consent pursuant to sections 28 and 40 (1) (*d*) and there is no other legal ground for the processing;

(*c*) the data subject objects to the processing pursuant to section 48 and there are no overriding legitimate grounds for the processing;

(*d*) personal data has been unlawfully processed; or

(*e*) personal data has to be erased in compliance with a legal obligation to which the data controller is subject.

(2) Where the data controller has made personal data public and is obliged pursuant to subsection (1) to erase the personal data, the data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data controllers which are processing the personal data that the data subject has requested the erasure by such data controllers of any links to, or copy or replication of, the personal data.

(3) Subsections (1) and (2) shall not apply where processing is necessary —

(*a*) for exercising the right of freedom of expression and information;

(*b*) for compliance with a legal obligation to which the data controller is subject or for the performance of a duty carried out in the public interest or in the exercise of official authority vested in the data controller;

(*c*) for reasons of public interest in the area of public health pursuant to section 30 (2) (*g*) to (*h*) and (3);

(*d*) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes pursuant to sections 30, (2) (*i*) and 35, insofar as the right referred to in subsection (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(*e*) for the establishment, exercise or defence of legal claims.

Right to restriction of processing

45. (1) The data subject shall have the right to obtain from the data controller restriction of processing where one of the following applies —

(*a*) the accuracy of the personal data is contested by the data subject:

Provided that the data controller is given a reasonable time to verify the accuracy of the personal data;

(*b*) processing is unlawful and the data subject opposes the erasure of the personal data, but requests the restriction of the use of personal data instead;

(*c*) the data controller no longer needs the personal data for the purpose of processing, but the data subject requires the personal data for the establishment, exercise or defence of legal claims pursuant to subsection (2) (*b*); or

(*d*) the data subject has objected to processing pursuant to section 48 (2) pending the verification whether the legitimate grounds of the data controller override those of the data subject.

(2) Where processing has been restricted under subsection (1), such personal data shall, with the exception of storage, only be processed —

(*a*) with the data subject's consent;

(*b*) for the establishment, exercise or defence of legal claims;

(*c*) for the protection of the rights of another natural or legal person; or

(*d*) in the public interest.

(3) A data subject who has obtained restriction of processing under subsection (1) shall be informed by the data controller before the restriction of processing is lifted.

Notification obligation for rectification or erasure of personal data or restriction of processing

46. (1) The data controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with section 43, 44 or 45 to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.

(2) The data controller shall, on a request made by the data subject, inform the data subject about the recipients under subsection (1).

Right to data portability

47. (1) The data subject shall have the right to receive personal data concerning him or her, which he or she has provided to a data controller, in a structured, commonly used and machine-readable format and have the right to transmit such data to another data controller without hindrance from the data controller to which the personal data has been provided, where —

(*a*) processing is based on consent or a contract pursuant to section 26 (*a*) or (*b*) or section 30 (2) (*a*); and

(*b*) processing is carried out by automated means.

(2) In exercising his or her right to data portability pursuant to subsection (1), the data subject shall, where technically feasible, have the right to have the personal data transmitted directly from one data controller to another.

(3) The exercise of the right in subsection (1) shall —

(*a*) be without prejudice to the right to erasure under section 44;

(*b*) not apply to processing necessary for the performance of a duty carried out in the public interest or in the exercise of official authority vested in the data controller; and

(*c*) not adversely affect the rights and freedoms of other persons.

Right to object

48. (1) The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him or her which is based on section 26 (*e*) or (*f*), including profiling based on those provisions.

(2) Where the data subject objects to processing pursuant to subsection (1), the data controller shall not process the personal data unless the data controller demonstrates compelling legitimate grounds for processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

(3) Where personal data is processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, including profiling related to such direct marketing.

(4) Where the data subject objects to processing for direct marketing purposes, his or her personal data shall not be processed for such purposes.

(5) At the time of the first communication with the data subject, the rights under subsections (1) and (2) shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

(6) Where personal data is processed for scientific or historical research purposes or statistical purposes pursuant to section 35 the data subject shall, on grounds relating to his or her particular situation, unless the processing is in public interest, have the right to object to processing of personal data concerning him or her.

Automated individual decision-making, including profiling

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

(2) Subsection (1) shall not apply if the decision is —

(*a*) necessary for entering into, or performance of, a contract between the data subject and a data controller under section 26 (*b*);

(*b*) based on the data subject's explicit consent under section 30 (2) (*a*); or

(*c*) authorised by a law under sections 26 (*c*) or 30 (2) (*f*).

(3) For purposes of subsection (2) (*a*) and (*b*), the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including the right to obtain human intervention on the part of the data controller, to express his or her point of view and to contest the decision.

PART IX — *Legal Restrictions*

Legal restrictions

50. (1) A law to which the data controller or data processor is subject may restrict the scope of the obligations and rights provided for in Parts VIII to X insofar as its provisions correspond to the rights and obligations provided for in Parts IV to VI.

(2) The restriction in subsection (1) shall respect the essence of the fundamental rights and freedoms and be a necessary and proportionate measure in a democratic society to safeguard —

(*a*) national security;

(*b*) public defence;

(*c*) public interest;

(*d*) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to national security;

(*e*) other objectives of general public interest, including —

(i) the economic or financial interest of Botswana,

(ii) monetary, budgetary and taxation matters, or

(iii) public health and social security;

(*f*) the protection of judicial independence and judicial proceedings;

(*g*) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(*h*) monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority under paragraphs (*a*) to (*e*) and (*g*);

(*i*) the protection of the data subject or the rights and freedoms of others; or

(*j*) the enforcement of legal claims.

(3) The measures under subsection (2) shall, where relevant, contain specific provisions relating to the —

(*a*) purpose of processing or categories of processing;

(*b*) categories of personal data;

(*c*) scope of the restrictions introduced;

(*d*) safeguards to prevent abuse or unlawful access or transfer;

(*e*) specification of the data controller or categories of data controllers;

(*f*) storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(*g*) risks to the rights and freedoms of data subjects; and

(*h*) right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

(4) In the event of any conflict or inconsistency between the provisions of this Act and any other legislation, the provisions of this Act shall take precedence insofar as the conflict or inconsistency relates to the obligations and rights under Parts IV to VI.

Responsibility of data controller

51. (1) The data controller shall, taking into account the nature, scope, context and purposes of processing and the risks of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the provisions of this Act.

(2) The measures in subsection (1) shall where —

(*a*) proportionate in relation to processing activities, include the implementation of appropriate data protection policies by the data controller; and

(*b*) necessary, be reviewed and updated.

(3) Pursuant to subsection (1), the data controller may use adherence to an approved code of conduct under section 73 to demonstrate compliance with the obligations of the data controller under this Act.

Data protection by design and by default

52. (1) The data controller shall, at the time of the determination of the means for processing and the time of the processing, taking into account the state of the art, cost of implementation and the nature, scope, context and purpose of processing and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, implement appropriate technical and organisational measures, designed to —

(*a*) implement data protection principles under Part IV in an effective manner; and

(*b*) integrate the necessary safeguards into the processing in order to meet the requirements of this Act and protect the rights of data subjects.

(2) The data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.

(3) The obligation in subsection (2) shall apply to the amount of personal data collected, the extent of the processing of that personal data, and the period of storage and accessibility of that personal data:

Provided that such measures shall ensure that, by default, personal data is not made accessible without human intervention to an indefinite number of natural persons.

Joint data controllers

53. (1) Where two or more data controllers jointly determine the purpose and means of processing, they shall be joint data controllers.

(2) The joint data controllers shall, in a transparent manner and by means of an arrangement between them, unless the respective responsibilities of the data controllers are determined by law in terms of section 52, determine their respective responsibilities —

(*a*) for compliance with the obligations under this Act; and

(*b*) as regards the exercising of the rights of the data subject and their respective duties to provide the information under Parts VIII to XI.

(3) The joint data controllers may, in the arrangement under subsection (2), designate a contact point for data subjects.

(4) The arrangement in subsection (2) shall —

(*a*) duly reflect the respective roles and relationships of the joint data controllers in relation to the data subjects; and

(*b*) be made available to the data subject.

(5) Notwithstanding the terms of the arrangement in this section, the data subject may exercise his or her rights under this Act in respect of and against each of the data controllers.

Representatives of controllers or processors not established in Botswana

54. (1) Where section 4 (2) applies, the controller or the processor shall designate in writing a representative in Botswana.

(2) The obligation laid down in subsection (1) shall not apply to —

(*a*) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in section 30 or processing of personal data relating to criminal convictions and offences referred to in section 32, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(*b*) a public authority or body.

(3) A representative shall be established in Botswana where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.

(4) A representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Act.

(5) The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

Data processor

55. (1) Where processing is carried out on behalf of a data controller, the data controller shall use only a data processor who provides sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing shall meet the requirements under section 62.

(2) The data processor shall not engage another data processor without prior specific or general written authorisation of the data controller.

(3) In the case of a general written authorisation, the data processor shall, giving the data controller the opportunity to object to such changes, inform the data controller of any intended changes concerning the addition or replacement of other data processors.

Data processor governed by contract or law

56. (1) Processing by a data processor shall be governed by a contract or law, that is binding on the data processor with regard to the data controller and that sets out the —

(*a*) subject-matter and duration of processing;

(*b*) nature and purpose of processing;

(*c*) type of personal data and categories of data subjects; and

(*d*) obligations and rights of the data controller.

(2) The contract or law in subsection (1) shall, in particular, provide that the data processor —

(*a*) processes the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to a third country or an international organisation, unless the data processor processes the personal data in terms of section 50:

Provided that where processing is carried out in terms of section 50, the data processor shall inform the data controller of any restriction before processing;

(*b*) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(*c*) respects the conditions under section 53 (2) and (3) for engaging another data processor;

(*d*) takes all measures required pursuant to section 62;

(*e*) taking into account the nature of the processing, assists the data controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the data controller's obligations set out in Parts VIII to IX;

(*f*) taking into account the nature of processing and the information available to the data processor, assists the data controller in ensuring compliance with the obligations under Parts XI and XII;

(*g*) at the choice of the data controller, deletes or returns all the personal data to the data controller after the end of the provision of services relating to processing, and deletes existing copies unless the law requires storage of the personal data; and

(*h*) makes available to the data controller all information necessary to demonstrate compliance with the obligations under this section and allow for and contribute to audits, including inspections, conducted by the data controller or an auditor authorised by the data controller.

(3) For the purposes of subsection (2) (*h*), the data processor shall immediately inform the data controller if, in its opinion, an instruction contravenes this Act.

Data processor engaging another data processor

57. (1) Where, with the approval of the data controller, a data processor engages another data processor for carrying out specific processing activities on behalf of the data controller pursuant to section 55 (2) and (3), the data protection obligations set out in Part IV shall be imposed on that other data processor by way of a contract or law, as may be applicable.

(2) Where the other data processor fails to fulfil its data protection obligations, the initial data processor shall remain fully liable to the data controller for the performance of that other data processor's obligations.

(3) The provisions of sections 58 to 61 shall, with the necessary modifications, apply to a data processor.

(4) Adherence of a data processor to a code of conduct approved pursuant to section 73 may be used to demonstrate compliance with the measures and obligations under sections 52 and 57.

Contract to be in writing

58. (1) Without prejudice to an individual contract between the data controller and the data processor, the contract or law under section 56 may be based, in whole or in part, on standard contractual clauses under section 59.

(2) The contract shall be in writing, including in electronic form.

(3) Without prejudice to sections 81 to 84, where a data processor determines the purposes and means of processing in contravention of the provisions of this section, the data processor shall be considered a data controller in respect of that processing.

Standard contractual clauses

59. (1) The Commission may lay down standard contractual clauses for purposes of section 57.

(2) A data controller may, for purposes of section 57, adopt standard contractual clauses under subsection (1).

Record of processing activities

60. (1) Each data controller and, where applicable, the controller's representative shall maintain a record of processing activities under its responsibility.

(2) The record in subsection (1) shall contain the following information —

(*a*) the name and contact details of the data controller and, where applicable, the joint data controllers, the controllers representative and the data protection officer;

(*b*) the purpose of processing;

(*c*) a description of the categories of data subjects and of the categories of personal data;

(*d*) the categories of recipients to whom the personal data is or will be disclosed including recipients in third countries or international organisations;

(*e*) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfer under section 80, the documentation of suitable safeguards;

(*f*) where possible, the envisaged time limits for erasure of the different categories of data; and

(*g*) where possible, a general description of the technical and organisational measures under section 62.

(3) A data processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a data controller, containing —

(*a*) the name and contact details of the data processor or data processors and of each data controller on behalf of which the data processor is acting, and where applicable the controller or processor's representative the data protection officer;

(*b*) the categories of processing carried out on behalf of each data controller;

(*c*) where applicable, information under subsection (2); and

(*d*) where possible, a general description of the technical and organisational measures under section 62.

(4) The records in subsections (1) and (3) shall be in writing, including in electronic form:

Provided that the obligations in subsections (1) and (3) shall not apply to an enterprise or organisation employing less than 250 persons unless the processing it carries out —

(i) is likely to result in a risk to the rights and freedoms of data subjects,

(ii) is not occasional, or

(iii) includes sensitive personal data in terms of section 30 (1) or personal data relating to criminal convictions or offences under section 32.

(5) The data controller or data processor and, where applicable, the controller or processor's representative shall make the record available to the Commission on request.

Cooperation with Commission

61. The data controller and data processor and where applicable their representatives shall cooperate, on request, with the Commission in the performance of its duties.

PART XI — *Security of Personal Data*

Appropriate technical and organisational measures

62. (1) The data controller and the data processor shall, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate —

(*a*) the pseudonymisation or encryption of personal data;

(*b*) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(*c*) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

(*d*) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2) In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, including accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(3) Adherence to an approved code of conduct under section 73 may be used to demonstrate compliance with the requirements set out in this section.

(4) The data controller and data processor shall take steps to ensure that any natural person acting under the authority of the data controller or the data processor who has access to personal data does not process them except on instructions from the data controller, unless he or she is required to do so by law under section 50.

Notification of personal data breach

63. (1) In the case of a personal data breach, the data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commission, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the data subject.

(2) Where the notification under subsection (1) is not made within 72 hours, it shall be accompanied by reasons for the delay.

(3) The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.

(4) The notification under subsection (1) shall —

(*a*) describe the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(*b*) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(*c*) describe the likely consequences of the personal data breach; and

(*d*) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(5) Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(6) The data controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

(7) The documentation in subsection (5) shall be provided in such manner as to enable the Commission to verify compliance with this section, as the Commission may determine.

Communication of personal data breach to data subject

64. (1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject under subsection (1) shall describe in clear and plain language the nature of the personal data breach and contain the information and measures under section 63 (4) (*b*) to (*d*).

(3) The communication to the data subject under subsection (1) shall not be required if any of the following conditions are met —

(*a*) the data controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(*b*) the data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects in subsection (1) is no longer likely to materialise; or

(*c*) it would involve disproportionate effort:

Provided that there shall, instead, be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

(4) Where the data controller fails to inform the data subject of the personal data breach, the Commission, having considered the likelihood of the personal data breach resulting in a high risk, may require the data controller to do so or may decide that any of the conditions under subsection (3) are nonetheless met.

PART XII — *Data Protection Impact Assessment and Prior Consultation*

Data protection impact assessment

65. (1) Where a type of processing uses new technologies, and taking into account the nature, scope, context and purpose of processing, is likely to result in a high risk to the rights and freedoms of natural persons, the data controller shall, prior to processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data:

Provided that a single assessment may address a set of similar processing operations that present similar high risks.

(2) The data controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

(3) A data protection impact assessment under subsection (1) shall be required where —

(*a*) a systematic and extensive evaluation of personal aspects relating to natural persons is based on automated processing, including profiling, and decisions that produce legal effects concerning the natural person or significantly affect the natural person;

(*b*) processing of sensitive personal data or personal data relating to criminal convictions and offences under section 30 or 32 is carried out on a large scale; or

(*c*) a systematic monitoring of a publicly accessible area is carried out on a large scale.

List of processing operations subject to data protection impact assessment

66. (1) The Commission shall establish and publish a list of processing operations for which a data protection impact assessment is required.

(2) Notwithstanding subsection (1), the Commission may establish and publish a list of processing operations for which no data protection impact assessment is required.

Contents of data protection impact assessment

67. (1) The data protection impact assessment shall contain, at least —

(*a*) a systematic description of the envisaged processing operations and the purpose of processing, including, where applicable, the legitimate interest pursued by the data controller;

(*b*) an assessment of the necessity and proportionality of the processing operations in relation to the purpose;

(*c*) an assessment of the risks to the rights and freedoms of data subjects under section 65; and

(*d*) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act taking into account the rights and legitimate interests of data subjects and other persons concerned.

(2) Compliance with approved codes of conduct under section 73 by a data controller or data processor shall be taken into account when assessing the impact of processing operations performed by such data controller or data processor.

(3) The data controller may, where appropriate and without prejudice to the protection of commercial or public interests or the security of processing operations, seek the views of data subjects or their representatives on the intended processing.

(4) Sections 65 to 67 shall not apply where —

(*a*) processing is carried out pursuant to section 26 (*c*) or (*e*), and the law regulates the specific processing operation or set of operations in question; and

(*b*) a data protection impact assessment has been carried out as part of a general impact assessment in the context of the adoption of that law.

(5) The data controller shall, when there is a change in the risk represented by processing operations, carry out a review of the risk in accordance with section 65.

Prior consultation

68. (1) Where a data protection impact assessment under section 65 indicates that, in the absence of measures to mitigate the risk, processing would result in a high risk, the data controller shall consult the Commission prior to processing.

(2) Where the Commission considers that the intended processing under subsection (1) would contravene this Act, and that the data controller has insufficiently identified or mitigated the risk, the Commission —

(*a*) shall, within eight weeks of receipt of the request for consultation, provide written advice to the data controller or data processor; and

(*b*) may exercise any of its powers under sections 14 to 17.

(3) The Commission may extend the period under subsection (2) by six weeks, taking into account the complexity of the intended processing.

(4) The Commission shall inform the data controller or data processor of the extension under subsection (3), and the reasons for delay, within one month of receipt of the request for consultation.

(5) The periods under subsections (2) to (4) may be suspended until the Commission has obtained information under subsection (6).

(6) When consulting the Commission, the data controller shall provide the Commission with the —

(*a*) respective responsibilities of the data controller, joint data controllers and data processors involved in the processing within a group of undertaking;

(*b*) purpose and means of the intended processing;

(*c*) measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to section 62;

(*d*) contact details of the data protection officer, where applicable;

(*e*) data protection impact assessment in terms of section 65; and

(*f*) other information requested by the Commission.

PART XIII — *Data Protection Officer*

Designation of data protection officer

69. (1) The data controller and the data processor shall designate a data protection officer where —

(*a*) processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(*b*) the core activities of the data controller or data processor consist of processing operations which, by virtue of their nature, scope and purpose, require regular and systematic monitoring of data subjects on a large scale; or

(*c*) the core activities of the data controller or data processor consist of processing of —

(i) sensitive personal data on a large scale; or

(ii) personal data relating to criminal convictions and offences under section 32.

(2) In cases other than those under subsection (1), a data controller or data processor or an association representing categories of data controllers or data processors may designate a data protection officer to act for the association:

Provided that the data controller shall display the contact details of the data protection officer in the premises and inform the Commission, in writing, of such contact details.

Qualification for designation

70. (1) A data protection officer shall be designated on the basis of —

(*a*) professional qualities, expert knowledge on data protection law and practices; and

(*b*) proven ability to fulfil duties under section 72.

(2) The data protection officer may be a staff member of the data controller or data processor, or may fulfil the duties on the basis of a service contract.

(3) Upon designation, the data controller or data processor shall submit the name and contact details of the data protection officer to the Commission in such manner as may be prescribed.

Position of data protection officer

71. (1) The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those duties and he or she shall not be dismissed or penalised by the controller or the processor for performing his or her duties.

(2) The data protection officer shall directly report to the highest management level of the data controller or the data processor.

(3) Pursuant to subsection (1), the data controller and data processor shall —

(*a*) ensure that the data protection officer is, properly and in a timely manner, involved in all issues relating to the protection of personal data;

(*b*) support the data protection officer in performing the duties under section 72 by providing the resources necessary to —

(i) carry out those duties and access to personal data and processing operations, and

(ii) maintain the data protection officer's expert knowledge; and

(*c*) ensure that the data protection officer has functional independence.

(4) Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Act.

(5) The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her duties.

(6) The data protection officer may, in addition to the duties under section 72 carry out other functions of the data controller or data processor:

Provided such functions and duties do not result in a conflict of interest.

Duties of data protection officer

72. (1) The data protection officer shall —

(*a*) inform and advise the data controller or the data processor, including the officers of the data controller or data processor who carry out processing, of their obligations under this Act;

(*b*) monitor compliance with —

(i) this Act and data protection provisions provided for elsewhere in the law, and

(ii) the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of officers involved in processing operations and related audits;

(*c*) provide, upon request, advice on the data protection impact assessment and monitor its performance pursuant to sections 65 to 67;

(*d*) act as the contact point for the Commission on issues relating to processing, including the prior consultation under section 68; and

(*e*) consult or cooperate with Commission on any other matter as may be necessary for purposes of this Act.

(2) The data protection officer shall, in performing the duties under subsection (1), have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purpose of processing.

Code of conduct

73. (1) Data controllers or data processors, or an association or body representing a category of data controllers or data processors, may, taking into account the specific features of the various processing sectors and specific needs of micro, small and medium-sized enterprises, draw up a code of conduct to ensure the proper application of, and adherence to, this Act.

(2) The code of conduct in subsection (1) shall set out —

(*a*) the measures and standards for fair and transparent processing;

(*b*) the legitimate interests pursued by the data controller in a specific context;

(*c*) procedures for the collection of personal data and the means for protecting such data or pseudonymisation of personal data;

(*d*) the procedures for providing information to the public and to data subjects;

(*e*) the procedures for notification of personal data breaches to the Commission and communication of such personal data breaches to data subjects;

(*f*) the transfer of personal data to third countries or international organisations;

(*g*) dispute resolution procedures for resolving disputes between data controllers and data subjects with regard to processing; or

(*h*) any other matter as may be necessary to ensure the proper application of this Act.

(3 A code of conduct drawn up under subsection (1) shall be submitted to the Commission for approval.

(4) The Commission shall, upon approval, register and publish the code of conduct.

PART XIV — *Transfers of Personal Data to Third Countries or International Organisations*

General principle for transfers

74. In order to ensure that the level of protection of natural persons guaranteed by this Act is not undermined, any transfer of personal data from a data controller or data processor in Botswana to a data controller, data processor or other recipient in a third country or an international organisation, including onward transfer to another third country or international organisation, shall be carried out subject to the provisions of this Part:

Provided that a copy of the personal data being transferred remains in Botswana for the period of processing.

Transfers on basis of adequacy decision

75. (1) A transfer of personal data to a third country or an international organisation may take place where the —

(*a*) Commission decides that the third country, a territory or one or more specified sector within that third country, or the international organisation in question ensures an adequate level of protection; and

(*b*) Minister, on recommendation of the Commission and by Order published in the *Gazette*, designates the transfer of personal data to any country or international organisation listed in the Order.

(2) When assessing the adequacy of the level of protection, the Commission shall take into account the —

(*a*) relevant legislation and access of public authorities to personal data, including the —

(i) implementation of such legislation, data protection rules, professional rules and security measures,

(ii) rules for onward transfer of personal data to another third country or international organisation, and case-law, and

(iii) administrative and judicial redress for the data subjects whose personal data is being transferred, in the third country or international organisation concerned;

(*b*) existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, including adequate enforcement powers, for —

(i) assisting and advising the data subjects in exercising their rights, and

(ii) cooperation with the other supervisory authorities; and

(*c*) international commitments in relation to the protection of personal data that the third country or international organisation concerned has entered into and other obligations arising from —

(i) legally binding conventions or instruments, and

(ii) its participation in multilateral or regional systems.

(3) After assessing the adequacy of the level of protection pursuant to subsection (2), the Commission may decide by means of an implementing act that a third country, a territory or one or more specified sectors within the third country, or an international organisation ensures an adequate level of protection within the meaning of this section.

(4) The implementing act in subsection (3) shall —

(*a*) subject to subsections (5) and (6) provide for a mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation;

(*b*) specify its territorial and sectorial application and, where applicable, identify the supervisory authority in subsection (2) (*b*); and

(*c*) be adopted in such form and manner as may be prescribed.

(5) The Commission shall, on an ongoing basis, monitor developments in third countries and international organisations that could affect the decision adopted pursuant to subsection (3).

(6) Where available information reveals that a third country or an international organisation no longer ensures an adequate level of protection within the meaning of this section, the Commission shall, to the extent necessary, repeal, amend or suspend the decision in subsection (3):

Provided that the Commission may enter into consultations with the third country or international organisation with a view to remedying the situation giving rise to the decision made pursuant to this subsection.

(7) A decision pursuant to subsection (3) shall be without prejudice to transfers of personal data to the third country or the international organisation in question pursuant to section 76.

(8) The Commission shall publish, on its website or such medium as it may determine, a list of third countries and international organisations designated in terms of subsection (1).

Transfers subject to appropriate safeguards

76. (1) In the absence of an adequacy decision pursuant to section 75, a data controller or data processor may transfer personal data to a third country or an international organisation —

(*a*) only if the data controller or data processor has provided appropriate safeguards; and

(*b*) on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

(2) The appropriate safeguards under subsection (1) may be provided for, without requiring any specific authorisation from the Commission, by —

(*a*) a legally binding and enforceable instrument between public authorities;

(*b*) binding corporate rules in accordance with section 77;

(*c*) standard data protection clauses adopted by the Commission; or

(*d*) an approved code of conduct pursuant to section 73, including binding and enforceable commitments of the data controller or data processor in the third country to apply the appropriate safeguards.

(3) The appropriate safeguards under subsection (1) shall require specific authorisation from the Commission if provided for by —

(*a*) contractual clauses between the data controller or data processor and the data controller, data processor or the recipient of the personal data in the third country or international organisation; or

(*b*) provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Binding corporate rules

77. (1) The Commission shall approve binding corporate rules:

Provided that the rules —

(i) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees,

(ii) expressly confer enforceable rights on data subjects with regard to the processing of their personal data, and

(iii) fulfil the requirements laid down in subsection (2).

(2) The binding corporate rules under subsection (1) shall specify —

(*a*) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(*b*) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(*c*) their legally binding nature, both internally and externally;

(*d*) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(*e*) the rights of data subjects in regard to processing and the means to exercise those rights and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(*f*) the acceptance by the data controller or data processor for any breach of the binding corporate rules;

(*g*) the duties of any data protection officer designated in accordance with section 69 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, including monitoring training and complaint handling;

(*h*) the complaint procedures;

(*i*) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules:

Provided that —

(i) such mechanisms include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject,

(ii) the results of such verification are communicated to the data protection officer person or entity under paragraph (*g*) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and

(iii) such mechanisms and the results of verification are available, upon request, to the Commission;

(*j*) the mechanisms for reporting and recording changes to the rules and reporting those changes to the Commission;

(*k*) the cooperation mechanism with the Commission to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity;

(*l*) the mechanisms for reporting to the Commission any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(*m*) the appropriate data protection training to personnel having permanent or regular access to personal data.

(3) The Commission may specify the format and procedures for the exchange of information between data controllers and data processors for binding corporate rules.

Derogations for specific situations

78. (1) In the absence of an adequacy decision, appropriate safeguards or binding corporate rules, a transfer of personal data to a third country or an international organisation shall take place on one of the following conditions —

(*a*) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

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

(*c*) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person;

(*d*) the transfer is necessary in the public interest;

(*e*) the transfer is necessary for the establishment, exercise or defence of legal claims;

(*f*) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(*g*) the transfer is made from a register which according to the law is intended to provide information to the public and which is open to consultation by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by the law for consultation are fulfilled in the particular case; or

(*h*) the transfer is necessary for the purpose of compelling legitimate interests pursued by the data controller which are not overridden by the interests or rights and freedoms of the data subject.

(2) A transfer pursuant to subsection (1) (*g*) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register:

Provided that where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

(3) Subsection (1) (*a*), (*b*), (*c*) and (*h*), and subsection (2), shall not apply to activities carried out by public authorities in the exercise of their official duties.

(4) The data controller or data processor shall document the assessment and the appropriate safeguards under subsection (1) (*a*) in the records under section 62.

International cooperation

79. The Commission shall, in relation to third countries and international organisations take appropriate steps to —

(*a*) develop international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data;

(*b*) engage relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data; and

(*c*) promote the exchange and documentation of personal data protection legislation and practice, including on jurisdictional conflicts with third countries.

PART XV — *Compensation, Administrative Fines and Penalties*

Right to lodge complaint with Commission

80. (1) Without prejudice to any other administrative or judicial remedy, a data subject shall have the right to lodge a complaint with the Commission if the data subject considers that the processing of personal data relating to him or her contravenes this Act.

(2) The Commission shall inform the complainant on the progress and the outcome of the complaint.

Right to compensation and liability

81. (1) Any person who suffers material or non-material damage as a result of a contravention of this Act, shall have the right to receive compensation from the data controller or data processor for the damage suffered.

(2) Any data controller involved in processing shall be liable for the damage caused by processing which contravenes this Act.

(3) A data processor shall be liable for the damage caused by processing where the data processor has —

(*a*) not complied with obligations specifically directed to the data processor under this Act; or

(*b*) acted outside or contrary to lawful instructions of the data controller.

(4) Where more than one data controller or data processor, or both a data controller and a data processor, are involved in the same processing and are responsible for any damage caused by processing, each data controller or data processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

(5) Where a controller or processor has, in accordance with subsection (4), paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers and processors involved in the same processing that part of the compensation corresponding to their part of their part of responsibility for the damage, in accordance with conditions set out in subsection (3).

General conditions for imposing administrative fines

82. (1) The Commission shall ensure that the imposition of an administrative fine in respect of any contravention of this Act shall in each individual case be effective, proportionate and dissuasive.

(2) An administrative fine under subsection (1) shall be —

(*a*) imposed in addition to the corrective measures under section 16; and

(*b*) in addition to and not in derogation of any criminal liability under this Act.

(3) When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine, the Commission shall consider —

(*a*) the nature, gravity and duration of the contravention taking into account the nature, scope or purpose of the processing concerned, and the number of data subjects affected and the level of damage suffered by them;

(*b*) the intentional or negligent character of the contravention;

(*c*) any action taken by the data controller or data processor to mitigate the damage suffered by data subjects;

(*d*) the degree of responsibility of the data controller or data processor taking into account technical and organisational measures implemented by them;

(*e*) any relevant previous contraventions by the data controller or data processor;

(*f*) the degree of cooperation with the Commission, in order to remedy the contravention and mitigate the possible adverse effects of the contravention;

(*g*) the categories of personal data affected by the contravention;

(*h*) the manner in which the contravention became known to the Commission, in particular whether, and if so to what extent, the data controller or data processor notified the contravention;

(*i*) where corrective measures under section 16 have previously been ordered against the data controller or data processor concerned with regard to the same subject-matter, compliance with those measures;

(*j*) adherence to approved codes of conduct; and

(*k*) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the contravention.

Gravity of contravention and administrative fines

83. (1) Where a data controller or data processor intentionally or negligently, for the same or linked processing operations, contravenes several provisions of this Act, the total amount of the administrative fine shall not exceed the amount specified in subsection (2) for the gravest contravention.

(2) An administrative fine not exceeding P10 000 000, or in the case of an undertaking, not exceeding two per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, shall apply to a contravention of the obligations of the data controller and data processor under sections 29 and 52.

(3) An administrative fine not exceeding P50 000 000, or in the case of an undertaking, not exceeding four per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher, shall apply to a contravention of —

(*a*) the basic principles for processing, including conditions for consent, under Parts IV to VI;

(*b*) the data subjects' rights under Part VIII;

(*c*) the transfers of personal data to a recipient in a third country or an international organisation under Part XIV;

(*d*) any obligations pursuant to law adopted under Part VII;

(*e*) an order or a temporary or definitive restriction on processing or the suspension of data flows by the Commission under section 16 (*f*) or failure to provide access in contravention of section 14 (*d*) and (*e*); and

(*f*) an order by the Commission under section 16.

Offences and penalties

84. (1) Where a data controller does not implement the security safeguards under Part XI, 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.

(2) A person who sells personal data commits an offence and is liable to a fine of P500 000 or to a term of imprisonment not exceeding nine years, or to both.

(3) A person who contravenes a provision of this Act commits an offence and is liable, where a penalty is not provided for, to a fine not exceeding P500 000 or to imprisonment for a term not exceeding nine years, or to both.

PART XVI — *Continuation of Appeals Tribunal*

Continuation of Appeals Tribunal

85. The Information and Data Protection Appeals Tribunal as established under the repealed Act shall continue to exist as if established under this Act.

Composition of Tribunal

86. (1) The Minister shall appoint, as a member of the Tribunal —

(*a*) a President, who shall be a legal practitioner who qualifies to be appointed as a High Court judge;

(*b*) a Vice President who shall be a legal practitioner who qualifies to be appointed as a High Court judge;

(*c*) three other persons who have knowledge and experience in the areas of data protection and access to information laws; and

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

(2) A person shall not qualify for appointment as a member of the Tribunal if he or she is an employee of the Commission.

(3) The Minister may, where he or she is satisfied that a person meets the requirements to be appointed under subsection (1), appoint a person to sit on the Tribunal as an alternate to any of the substantive member of the tribunal appointed under subsection (1).

(4) The Minister shall by notice in the *Gazette*, publish the appointments of members of the Tribunal or their alternates, specifying the dates of their appointments and the period for which they are appointed.

Jurisdiction of Tribunal

87. (1) The Tribunal shall adjudicate over matters brought before it for breach of any of the provisions of this Act.

(2) Without prejudice to the generality of subsection (1), the Tribunal shall have the jurisdiction to —

(*a*) consider appeals lodged by a —

(i) data subject or his or her representative,

(ii) parent, guardian or carer, in the case of the data subject who is a minor or a person with disability, or

(iii) data controller, against any action or decision of the Commissioner; or

(*b*) review any decision of the Commissioner brought before it by —

(i) a data subject, or

(ii) a parent or guardian in the case of a minor or a person with physical or mental impairment.

(2) In taking decisions, the Tribunal shall exercise its discretion with independence and impartiality.

Tenure of office for members of Tribunal

88. The President and other members of the Tribunal shall hold office for a period not exceeding five years, and shall be eligible for re-appointment for only one further term not exceeding five years.

Disqualification, suspension and removal of member of Tribunal

89. (1) A person shall not qualify for appointment as a member or continue to hold office, if he or she —

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

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

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

(*b*) has, within a period of ten years immediately preceding the date of his or her proposed appointment, been convicted —

(i) in Botswana, of a criminal offence which has not been overturned on appeal or in respect of which he or she has not received a free pardon, or

(ii) outside Botswana, of an offence, which in Botswana, would have been a criminal offence,

and sentenced by a court of competent jurisdiction to imprisonment for one month or more without the option of a fine, whether that sentence has been suspended or not, and which conviction has not been overturned on appeal and in respect of which he or she has not received a free pardon.

(2) The Minister may suspend from office, a member against whom criminal proceedings are instituted for an offence in respect of which a sentence of imprisonment without an option of a fine may be imposed, and while the member is so suspended, such member shall not carry out any functions under this Act or be entitled to any remuneration or allowances.

(3) The Minister shall remove a member from office, if the member —

(*a*) becomes subject to a disqualification under subsection (1);

(*b*) contravenes a provision of this Act or otherwise misconducts himself or herself to the detriment of the functions of the Tribunal;

(*c*) has been convicted of an offence under this Act, or under any other Act and after a period of 30 days from the date that a ruling against the member is made on all appeals made in respect of the conviction, he or she is sentenced to imprisonment for a term of six months or more without an option of fine;

(*d*) is absent, without reasonable cause, from three consecutive meetings of which that member has had notice; or

(*e*) is found to be physically and mentally incapable of performing his or her duties efficiently, and a medical doctor has issued a medical certificate to that effect.

Vacation of office by member of Tribunal

90. A member shall vacate his or her office and such office shall become vacant —

(*a*) if he or she is disqualified, suspended or removed, in terms of section 89;

(*b*) if he or she is adjudged bankrupt or insolvent;

(*c*) upon his or her death;

(*d*) upon the expiry of such time as the Minister may specify in writing, notifying the member of his or her removal from office by the Minister;

(*e*) upon the expiry of one month's notice in writing to the Minister of his or her intention to resign from office;

(*f*) if he or she becomes physically or mentally incapable of performing his or her duties efficiently and a medical doctor has issued a medical certificate to that effect;

(*g*) if he or she is convicted of an offence under this Act or any other Act for which he or she is sentenced to imprisonment for a term of six months or more without an option of a fine; or

(*h*) if he or she is summarily dismissed from the Tribunal by the Minister for contravening this Act.

Resignation from Tribunal

91. A member may resign from his or her appointment by giving one month's notice, in writing, to the Minister.

Filling of vacancy

92. (1) Where the office of a member becomes vacant before the expiry of the member's term of office due to death, resignation or removal from office, the Minister shall, in accordance with section 89 of this Act and within four months from the date the vacancy occurs, appoint another person to be a member.

(2) The person appointed under subsection (1) shall —

(*a*) take the place of the member who has vacated office; and

(*b*) be appointed on a new or full term.

(3) Notwithstanding subsection (2), a person appointed under subsection (1) may hold office for such period as the Minister may, subject to section 88, specify.

Remuneration of members of Tribunal

93. A member of the Tribunal shall be paid such remuneration and allowances as the Minister may determine.

Appointment of Registrar of Tribunal

94. (1) The Minister shall appoint a Registrar and such other employees of the Tribunal as may be necessary, who shall provide secretarial services to the Tribunal.

(2) The Registrar shall —

(*a*) register all orders and decisions made by the Tribunal;

(*b*) maintain and keep a proper record of all proceedings and correspondence of the Tribunal;

(*c*) compile and register statistics of all adjudicated cases; and

(*d*) carry out such other duties as the Minister may, from time to time, determine.

Appeals to Tribunal

95. (1) A person who is aggrieved by a decision of the Commissioner under this Act or the Access to Information Act may, within 30 days of such decision, appeal to the Appeals Tribunal.

(2) In determining an appeal, the Tribunal may —

(*a*) dismiss the appeal; or

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

Proceedings of Tribunal

96. (1) The Tribunal shall sit as and when it receives 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.

Appeal against decision of Tribunal

97. A party who is aggrieved by the decision of the Tribunal may appeal to the High Court against such decision.

PART XVII — *Miscellaneous Provisions*

Protection from personal liability

98. No matter or thing done or omitted to be done by the Commissioner, Deputy 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, Deputy Commissioner or officer or any person acting under the direction of the Commissioner, personally liable to an action, claim or demand.

Regulations

99. 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.

Repeal of Cap. 43:14

100. The Data Protection Act is hereby repealed.

Transitional and savings provisions

101. (1) Notwithstanding the effect of the repeal under section 100, any subsidiary legislation made under the repealed Act, and in force immediately prior to the coming into operation of this Act shall, insofar as such legislation is consistent with the provisions of this Act, continue to be in force as if made under this Act.

(2) Any legal proceedings which, before the coming into operation of this Act, were pending shall be continued or enforced by or against the Commission in the same manner as they would have been continued or enforced before the coming into operation of this Act.

(3) Any investigations commenced under the repealed Act shall continue as if made under this Act.

(4) Any decisions made under the repealed Act shall be binding as if they were made under this Act.

(5) Any appeal or disciplinary proceedings which, prior to the coming into operation of this Act, were pending shall be continued as if they would have been continued before the coming into operation of this Act.

(6) The administrative structures of the Commission in existence under the repealed Act immediately before the commencement of this Act shall, to the extent that their continued existence is not inappropriate or inconsistent with this Act, continue in existence.

(7) Any person who is an officer or employee of the Commission immediately before the coming into operation of this Act shall continue in office for the period for which, and be subject to the conditions under which, he or she was appointed.

PASSED by the National Assembly this 19th day of August, 2024.

BARBARA N. DITHAPO,
Clerk of the National Assembly.