GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$	WINDHOEK	NO.

CONTENTS

Government Notice

MINISTRY OF INFORMATION AND COMMUNICATION TECHNOLOGY

No. ….. **2022**

PUBLICATION OF REVISED VERSION OF DRAFT BILL

The following version of the Draft Bill has been prepared and issued by the Minister of Information and Communication Technology and is hereby published for public comment(s).

_____

DRAFT DATA PROTECTION BILL

ACT

To establish a Data Protection Supervisory Authority and to provide for its powers, duties and functions; to establish obligations of data controllers and processors; to make provision for the regulation of the processing of information relating to individuals in order to protect the fundamental rights and freedoms of individuals, and in particular, their right to privacy concerning the processing of such information; to provide for the rights of individuals about whom information is processed; to provide for restrictions and exceptions under the provisions of this Act; to provide for codes of conduct of controllers and processors and for matters connected therewith.

(TO BE) ENACTED by the Parliament of the Republic of Namibia as follows:

ARRANGEMENT OF ACT

PART 1

PRELIMINARY

PART 2

DATA PROTECTION SUPERVISORY AUTHORITY

PART 3

OBLIGATIONS OF CONTROLLERS AND PROCESSORS

PART 4

EXCEPTIONS

PART 5

CODES OF CONDUCT

PART 6

TRANSBORDER FLOWS OF PERSONAL DATA

PART 7

ENFORCEMENT

PART 8

GENERAL PROVISIONS

PART 1
PRELIMINARY

1. Definitions

For purposes of this Act:

“Authority”, means the Data Protection Supervisory Authority established by section 3.

“anonymisation” refers to the process applied to personal data so that the data subject can no longer be identified, either directly or indirectly;

“automated individual decision-making and profiling” means a decision based solely on automated processing, including profiling and shall only be carried out under PART II Section 11 of this Act;

“biometric data” means personal data relating to the physical, physiological, biological or behavioural characteristics of an individual which allows the unique identification or authentication of the individual including by facial images or dactyloscopic data;

"child", refers to a person who is under the legal age of majority in accordance with the law of Namibia;

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

"controller" means a natural or legal person or public body that alone or jointly with others ('joint-controllers'), has decision-making powers determining the purposes and means of the processing of personal data. Where the purposes and means of processing are determined by an act, decree or ordinance, the controller is a natural person, legal person or public body that has been designated as such by that act, decree or ordinance. The controller shall be responsible for the processing of personal data carried out on its behalf by a processor;

"data concerning health" means personal data that are related to the past, present or future physical or mental health of an individual, and which includes information relating to the provision of health care services which reveal information about the individual's health status;

"Data Protection Supervisory Authority"**,** refers to an independent public authority responsible for ensuring that personal data is processed in compliance with the provisions of this Act. This implies a decision-making power independent of any direct or indirect external influence on that Authority;

"data subject" means an identified or identifiable living individual to whom personal data relates. An "identified or Identifiable individual**"** means -

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

(b) in identifying whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person authorised by the controller to identify the said person; and

(c) an individual who is "identifiable" if the processing allows the individual to be 'singled out' from other individuals.

"direct marketing" means the communication of any advertising or marketing material which is directed to any particular individual;

"genetic data" means all data relating to the genetic characteristics of an individual which have been either inherited or acquired during prenatal development, as they result from an analysis of a biological sample from the individual concerned, in particular chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

"personal data" means any information relating to an identified or identifiable individual ('data subject'). An identifiable individual is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, a pseudonym, and IP address, location data, factors relating to the economic, mental, cultural, physical,

genetic, biometric or social identity and online identifier, and includes 'singling-out' an individual;

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

"processing" means any operation performed on personal data, and includes, the collection, recording, organisation, structuring, storage or preservation, combination, adaption or alteration, access, retrieval or consultation, transmission, disclosure or making available, restriction, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data;

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

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

"pseudonymisation" means the 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 and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

"recipient" means a person to whom data are disclosed or made available;

"responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

"restriction of processing" means the marking of stored personal data to limit their processing;

"special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning an individual's sex life or sexual orientation and personal data relating to criminal offences, including criminal records.

"third party" means any person, other than the data subject, the controller, the processor and anyone who, under the direct authority of the controller or the processor, is authorised to process the data.

2. Scope and Application of this Act

(1) This Act applies to the processing of personal data wholly or partly by automated and by non-automated means, where the personal data form part of a structured set of data and are accessible or retrievable according to specific criteria.

(2) This Act protects data subjects with regard to the processing of personal data by -

(a) requiring that personal data is processed in a transparent, fair and lawful manner, on the basis of an individual's consent or another specified lawful basis; and

(b) imposing conditions on data controllers or a person acting under their authority set out in **PART 3** including conditions of accountability, processing limitation, purpose specification, information quality, openness, security safeguards and access to personal data by data subject.

(3) This Act applies to the processing of personal data carried out by controllers, and where applicable processors and third parties.

(4) This Act applies to the processing of personal data done within and outside the territory of Namibia where the processing relates to individuals within the jurisdiction of Namibia.

(5) This Act does not apply to personal data processed by an individual in the course of a purely personal or household activity.

PART 2

DATA PROTECTION SUPERVISORY AUTHORITY

3. Establishment of Authority

There is established a juristic person to be known as the Data Protection Supervisory Authority, which –

(a) has jurisdiction throughout Namibia;

(b) is independent and subject only to the Namibian Constitution and the law;

(c) must be impartial and must perform its functions without fear, favour or prejudice; and

(d) must exercise its powers and perform its functions in accordance with this Act.

4. Powers of Authority

The Authority may –

(a) employ or otherwise engage persons to render services to the Authority or to otherwise assist it;

(b) acquire or hire such movable or immovable property as may be required for the effective performance of its functions, and dispose of property so acquired or hired;

(c) insure itself against any loss, damage, risk or liability which it may suffer or incur in good faith; and

(d) disseminate information to persons engaged in the processing of personal data and data subjects with respect to the provisions of this Act and the functions of the Authority;

(e) liaise and exchange information, knowledge and expertise with data protection authorities of other countries entrusted with functions similar to those of the Authority;

(f) carry out research into matters referred to the Authority by the Minister;

(g) advise the Minister on matters referred to the Authority by the Minister;

(h) be responsible for investigating contraventions of this Act by data controllers and any other person under the authority of the data controller; and

(i) advise the Minister, and any other person in relation to international agreements concerning personal data governed by this Act.

5. Duties and functions of Authority

(1) The duties and functions of the Authority in terms of this Act are to -

(a) consult with interested parties by –

(i) receiving and inviting representations from members of the public on any matter affecting personal data;

(ii) co-operating on a national and international basis with other persons and bodies concerned with the protection of personal data ; and

(iii) acting as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of personal data;

(b) handle complaints by –

(i) receiving and investigating complaints about alleged violations of the protection of personal data and reporting to complainants in respect of such complaints;

(ii) gathering such information as in the opinion of the Authority will assist the Authority in discharging the duties and carrying out the functions of the Authority under this Act;

(iii) attempting to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation; and

(iv) serving any notices in terms of this Act and further promoting the resolution of disputes in accordance with the prescripts of this Act;

(c) monitor and enforce compliance by –

(i) public and private bodies with the provisions of this Act;

(ii) undertaking research into, and monitoring developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of personal data is minimised, and reporting to the Minister the results of such research and monitoring;

(iii) examining any proposed legislation, including subordinate legislation, or proposed policy of the Government that the Authority considers may affect the protection of personal data, and reporting to the Minister the results of that examination;

(iv) conducting an assessment, on its own initiative, or when requested to do so, of a public or private body, in respect of the processing of personal data by that body for the purpose of ascertaining whether or not the data is processed according to the conditions for the lawful processing of personal data;

(v) monitoring the use of unique identifiers of data subjects, and reporting to the Minister from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative or other action to give protection, or better protection, to personal data;

(vi) examining any proposed legislation that makes provision for the collection of personal data by any public or private body;

(d) conduct research and report to the Minister –

(i) from time to time on the desirability of the acceptance by Namibia, of any international instrument relating to the protection of personal data;

(ii) on any other matter, including necessary legislative amendments, relating to the protection of personal data that, in the opinion of the Authority, must be drawn to the attention of the Minister;

(e) in, respect of codes of conduct –

(i) issue, from time to time, codes of conduct, amend codes of conduct and to revoke codes of conduct;

(ii) make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct; and

(iii) consider afresh, upon application, determination by adjudicators under approved codes of conduct;

(f) facilitate cross-border co-operation in the enforcement of privacy laws by participating in any initiative that is aimed at such cooperation;

(g) in general –

(i) do anything incidental or conducive to the performance of any of the functions of the Authority;

(ii) exercise and perform such other functions, powers, and duties as are conferred or imposed on the Authority by or under this Act or any other legislation; and

(iv) prepare the responsible party to disclose to any person affected by a compromise to the integrity of confidentiality of personal data;

(h) submit to the Court any administrative act which does not comply with the fundamental rights of the protection of the right to privacy and the protection of personal data;

(i) advise the Minister and other institutions and bodies on matters relating to the right to privacy and data protection and related fundamental rights;

(j) establish and maintain a list of processing operations that require a data protection impact assessment; and

(k) issue guidance on appropriate data protection measures and safeguards, implementation and demonstration of compliance with this Act;

(2) The performance of the tasks of the Authority is free of charge to data subjects.

6. Board of Authority

(1) The Authority must have a Board which, subject to this Act, is responsible for the policy, management and control of the affairs of the Authority.

(2) The Authority is a public enterprise as defined in the Public Enterprises Governance Act and its governance must, unless otherwise exempted under that Act, be structured and conducted in accordance with the provisions of that Act.

(3) The chief executive officer is an *ex officio* member of the Board and –

(a) in that capacity he or she is entitled to vote on matters relating to or concerning the performance of regulatory or supervisory functions or exercise of regulatory or supervisory powers by the Authority under this Act; but

(b) the chief executive officer may not serve as the chairperson of the Board.

(4) The Minister may appoint an alternate member for each member of the Board.

7. Appointment of members of Board

(1) The Board must be constituted by not more than five members and the members and alternate members, including the chairperson and the vice-chairperson of the Board, must be appointed in accordance with section 14 and 15 of the Public Enterprises Governance Act.

(2) In addition to any advice given to him or her pursuant to section 14(1)(c) of the Public Enterprises Governance Act, the Minister when appointing members or alternate members of the Board must –

(a) have due regard to the integrity and independence of the judicial system in Namibia and the public interest; and

(b) appoint persons with appropriate and relevant knowledge, skills and experience in particular in the following areas of education –

(i) information communication technology (ICT);

(ii) law

(iii) data protection policy

(iv) cybersecurity management

(v) finance or management sciences

(3) The Minister must, as soon as possible after an appointment has been made, publish in the *Gazette* the names of the individuals appointed as members and individuals appointed as alternate members of the Board and their dates of appointment.

(4) Despite subsection (3), a failure to publish the names pf members of alternate members of the Board pursuant to that subsection does not invalidate any actions or decision taken by the Board, if the members or alternate members were properly appointed.

8. Chairperson of Board

(1) The Minister must, subject to section 11, appoint a chairperson and a vice-chairperson from among the members of the Board.

(2) The chairperson or in his or her absence, the vice-chairperson must preside at a meeting of the Board.

(3) If both the chairperson and the vice-chairperson are for any reason unable to preside over a meeting of the Board, the members present must elect a member from among themselves to act as a chairperson of the Board.

9. Disqualification of appointment

(1) Subject to subsection (2), a person is not eligible for appointment as a member or an alternate member of the Board or as a chief executive officer, if that person –

(a) is not a Namibian citizen or is not lawfully admitted to Namibia for permanent residence;

(b) is a member of Parliament or a regional or local authority council, unless he or she ceases to be such a member before the date of the proposed appointment;

(c) is an office-bearer of any political party, unless he or she ceases to be such an office-bearer before the date of the proposed appointment;

(d) has during the period of 10 years immediately preceding the date of commencement of this Act or at any time after that date been convicted, whether in Namibia or elsewhere, of an offence and has been sentenced to imprisonment without the option of a fine;

(e) is an unrehabilitated insolvent;

(f) has under any law been declared to be of unsound mind or under legal disability;

(g) has been removed from an office of trust; or

(h) has been sanctioned by any national or international statutory regulatory body for the contravention of a law relating to the regulation and supervision of data protection.

(2) Despite subsection (1)(a), the Minister may, where he or she considers it necessary and subject to the Immigration Control Act, 1993 (Act No. 7 of 1993), appoint a person as a member or an alternate member of the Board who is not a Namibian citizen or lawfully admitted to permanent residency in Namibia.

10. Vacation of office and filling of vacancies

(1) A member vacates his or her office, if the member –

(a) is convicted of an offence and sentenced to imprisonment without the option of a fine;

(b) resigns his or her office by giving the Minister one month's notice in writing of his or her intention to resign;

(c) has been absent for three consecutive meetings of the Board without leave of the Board; or

(d) is removed from office by the Minister under subsection (2).

(2) The Minister may, by notice in writing, remove a member from office if the Minister, after giving the member a reasonable opportunity to be heard, is satisfied that the member –

(a) has failed to comply with any obligation imposed by section 11;

(b) is guilty of neglect of duty or misconduct; or

(c) is incapable of performing the duties of his or her office, by reason of physical or mental illness.

(3) If the office of a member becomes vacant, the vacancy must be filled by the appointment of another person as member for the unexpired portion of the term of office of the person who ceased to hold office.

11. Conduct of members and disclosure of interest

(1) A member of the Board may not –

(a) engage in an activity that may undermine the integrity of the Authority;

(b) participate in any investigation or decision concerning a matter in respect of which the member has a financial or other personal interest; or

(c) use any confidential information obtained in the performance of his or her functions as a member to obtain, directly or indirectly, a financial or other advantage for himself or herself or any other person.

(2) Every member of the Board must in writing disclose to the Minister any direct or indirect financial interest which the member has or acquires in any business carried on in Namibia or elsewhere or in any body corporate carrying on any business in Namibia or elsewhere.

(3) A member who has or acquires any financial or other personal interest, either directly or indirectly, in any matter which is before the Board for discussion and determination must –

(a) immediately and fully disclose the interest to the Board; and

(b) withdraw from any further discussion or determination by the Board of that matter.

12. Remuneration

The members of the Board must be paid such remuneration or allowances or other benefits as the Minister, with the concurrence of the Minister of Finance, may determine.

13. Staff of Authority

(1) The Authority must appoint a chief executive officer and may appoint other employees as it deems necessary to assist in the performance of the duties and functions of the Authority.

(2) The chief executive officer is, subject to the directions of the Board, responsible for –

(a) the formation and development of an efficient administration; and

(b) the organisation, control, management and discipline of the staff of the Authority.

(3) Unless the Authority directs otherwise, the chief executive officer must attend the meetings of the Board and of the Authority, and the chief executive officer has a vote.

(4) Subject to section 18(3) of the Public Enterprises Governance Act, 2019, the Board determines the remuneration and other conditions of service and benefits of the chief executive officer and other employees of the Authority.

14. Funds of Authority

(1) The funds of the Authority consist of –

(a) money appropriated by Parliament for the purposes of the Authority;

(b) money raised as fees, and interest on unpaid fees, in respect of services rendered by the Authority in the performance of its functions;

(c) levies imposed on data controllers and such persons acting under the authority of the controller;

(d) money vesting in or accruing to the Authority from any other source; and

(d) interest derived from the investment of funds of the Authority.

(2) The Authority must submit to the Minister annually, at a time determined by the Minister, a statement of the estimated income and expenditure of the Authority, and requested appropriation from Parliament, for its next financial year.

(3) Expenditure incurred for the performance of the functions of the Authority, including remuneration, allowances or other benefits payable to members or other persons, must be defrayed from the funds of the Authority.

(4) The chief executive officer is the accounting officer of the Authority and is responsible for –

(a) all income and expenditure of the Authority; and

(b) all assets and the discharging of all liabilities of the Authority.

15. Bank accounts

(1) The Authority must open and maintain such bank accounts at one or more banking institutions in Namibia, registered in terms of the Banking Institutions Act, 1998 (Act No. 2 of 1998) as are necessary for the performance of the functions of the Authority.

(2) The Authority must ensure that –

(a) all money received by or on behalf of the Authority is deposited into its bank account as soon as practicable after being received;

(b) any payment by or on behalf of the Authority is made from its bank account; and

(c) no money is withdrawn, paid or transferred from its bank account without the Board's authority.

(3) Payments drawn on the bank account of the Authority, or any other form or document to be completed for the withdrawal, payment or transfer of money from any of the bank accounts of the Authority, must be signed on behalf of the Authority by two persons authorised for that purpose by the Board.

16. Investment of money

Any money of the Authority that is not immediately required for expenditure by the Authority may be invested at a banking institution referred to in section 15(1) or a building society registered in terms of the Building Societies Act, 1986 (Act No. 2 of 1986).

17. Financial year, accounts and audit

(1) The financial year of the Authority is as prescribed.

(2) The Authority must cause such records of account to be kept in accordance with general accepted accounting practices, principles and procedures as are necessary to represent fairly the state of affairs and business of the Authority and to explain the transactions and financial position of the Authority.

(3) Not later than three months after the end of each financial year of the Authority, the chief executive officer must prepare and submit to the Board for approval, financial statements, comprising –

(a) a statement reflecting, with suitable and sufficient particulars, the income and expenditure of the Authority during that financial year; and

(b) a balance sheet showing the state of the assets, liabilities and financial position of the Authority as at the end of that financial year.

(4) The accounting records and the financial statements of the Authority must be audited annually by the Auditor-General.

18. Annual report

(1) The Authority must submit to the Minister an annual report of its activities within six months of the end of each financial year, or such longer period as the Minister may determine, which report must be accompanied by –

(a) the audited financial statements of the Authority for that financial year; and

(b) the report of the auditor relating to those financial statements.

(2) The Minister must lay upon the Table of the National Assembly the annual report and financial statements submitted to the Minister in terms of subsection (1) within 30 days from the date of their receipt or, if the National Assembly is not then in ordinary session, within 14 days after the commencement of its next ordinary session.

(3) The Authority must, if the Minister at any time so requires, furnish to the Minister a report and particulars relating to the performance of the functions of the Commission in relation to any matter as the Minister may require.

19. Cooperation with other Supervisory Authorities

The Data Protection Supervisory Authority must perform the data protection duties and functions that are necessary to give effect to any international obligations arising from international data protection instruments.

PART 3

OBLIGATIONS OF CONTROLLERS AND PROCESSORS

20. Lawfulness of processing

(1) Personal data must be processed –

(a) lawfully; and

(b) in a reasonable manner that does not infringe the privacy of the data subject.

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

(3) Personal data may only be processed if –

(a) the data subject or a competent person where the data subject is a child consents to the processing;

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

(c) processing complies with an obligation imposed by law on the controller;

(d) processing protects a legitimate interest of the data subject;

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

(f) the processing is necessary for pursuing the legitimate interests of the controller or a third party to whom the data is supplied, except where such interests may infringe on the interests, rights and freedoms the data subject and that which override those of the controller or third-party.

(g) the processing is carried out for archiving purposes in the public interest, or for scientific or historical research purposes or statistical purposes, subject to appropriate safeguards for the rights and freedoms of data subjects.

(4) Where the processing is carried out for a purpose which is not the original purpose for which the personal data was collected, the controller must carry out an assessment and take into account -

(a) the context in which the personal data were originally collected and the compatibility of the new purpose, and the reasonable expectations of the data subject;

(b) any link between the original purpose for which the personal data were collected and the intended additional processing of the personal data;

(c) the nature of the personal data to be processed, including any additional safeguards afforded, such as special categories of personal data or data related to criminal offences and convictions; and

(d) any possible consequences for the data subject including any prejudice or harm to the rights and freedoms of data subjects.

(5) (a) The controller or the third party to whom personal data is supplied bears the burden of proof for the consent of the data subject or the competent person referred to in subsection (3)(a).

(b) The data subject or competent person may withdraw his or her consent referred to in subsection (3)(a) at any time: Provided that the lawfulness of the processing of personal data before such withdrawal or the processing of personal data in terms of subsection (3)(b) to (f) will not be affected.

(6) A data subject may object, at any time, to the processing of personal data –

(a) in terms of subsection (3)(d) to (f), in the prescribed manner, on reasonable grounds relating to his or her particular situation, unless legislation provides for such processing; or

(b) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communication.

(7) If a data subject has objected to the processing of personal data in terms of subsection (6), the controller or a person acting under the authority of the controller, may no longer process the personal data.

(8) A controller or a person acting under the authority of a controller who unlawfully process personal data in contravention of this section commits an offence and is liable to pay a fine to the Authority as prescribed.

21. Collection directly from data subject

(1) Personal data must be collected directly from the data subject, except as otherwise provided for in subsection (2).

(2) It is not necessary to comply with subsection (1) if –

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

(b) the data subject or a competent person where the data subject is a child has consented to the collection of personal data from another source;

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

(d) collection of personal data from another source is necessary –

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the Namibia Revenue Agency Act, 2017 (Act No. 12 of 2017);

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

(iv) in the interests of national security; or

(v) to maintain the legitimate interests of the controller or of a third party to whom personal data is supplied.

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

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

22. Collection for specific purpose

(1) Personal data must be collected for specific, explicitly defined and lawful purpose related to a function or activity of the controller.

(2) Steps must be taken in accordance with section 27(1) to ensure that the data subject is aware of the purpose of the collection of the personal data unless the provisions of section 27(4) are applicable.

23. Retention and restriction of records

(1) Subject to subsections (2) and (3), records of personal data must not be retained any longer than is necessary for achieving the purpose for which the personal data was collected or subsequently processed, unless -

(a) retention of the record is required or authorised by law;
(b) the controller reasonably require the record for lawful purposes related to its functions or activities;
(c) retention of the record is required by a contract between the parties thereto; or
(d) the data subject or a competent person where the data subject is a child has consented to the retention of the record.

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

(3) A controller that has used a record of personal data of a data subject to make a decision about the data subject, must –

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

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

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

(5) The destruction or deletion of a record of personal data in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.

(6) The controller must restrict processing of personal data if –

(a) its accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the controller no longer needs the personal data for achieving the purpose for which the data was collected or subsequently processed, but it has to be maintained for purposes of proof;

(c) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

(d) the data subjects requests to transmit the personal data into another automated processing system.

(7) Personal data referred to in subsection (6) may, with the exception of storage, only be processed for purposes of proof, or with the consent of the data subject, or with the consent of the competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

(8) Where processing of personal data is restricted pursuant to subsection (6), the controller must inform the data subject before lifting the restriction on processing.

24. Further processing to be compatible with purpose of collection

(1) Further processing of personal data must be in accordance or compatible with the purpose for which it was collected in terms of section 22.

(2) To assess whether further processing is compatible with the purpose of collection, the controller must take into account –

(a) the relationship between the purpose of the intended further processing and the purpose for which the personal data has been collected;
(b) the nature of the data concerned;
(c) the consequences of the intended further processing for the data subject;
(d) the manner in which the data has been collected; and
(e) any contractual rights and obligations between the parties.

(3) The further processing of personal data is not incompatible with the purpose of collection if –

(a) the data subject or a competent person where the data subject is a child has consented to the further processing of the personal data;
(b) the personal data is available in or derived from a public record or has deliberately been made public by the data subject;
(c) further processing is necessary –
    (i) to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;
    (ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the Namibia Revenue Agency Act, 2017 (Act No. 12 of 2017);
    (iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or
    (iv) in the interests of national security;

(d) the further processing of personal data is necessary to prevent or mitigate a serious or imminent threat to -

(i) public health or public safety; or

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

(e) the personal data is used for historical, statistical or research purposes and the controller ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; and

(f) the further processing of the personal data is in accordance with an exemption granted under section 35.

25. Quality of information

(1) A controller or a person acting under the authority of the controller must take reasonable practical steps to ensure that the personal data is complete, accurate, not misleading and updated where necessary.

(2) In taking the steps referred to in subsection (1), the controller must have regard to the purpose for which personal data is collected and further processed.

26. Notification to data subject when collecting personal data

(1) If personal data is collected, the controller must take reasonably practical steps that the data subjects is aware of –

(a) the personal data being collected and where the personal data is not collected from the data subject, the source from which it is collected;

(b) the name and address of the controller;

(c) the purpose for which the personal data is being collected;

(d) whether or not the supply of the personal data by that data subject is voluntary or mandatory;

(e) the consequences or failure to provide the personal data;

(f) any particular law authorising or requiring the collection of the personal data;

(g) the fact that, where applicable, the controller intends to transfer the personal data to a third country or international organisation and the

level of protection afforded to the personal data by that third country or international organisation;

(h) any further processing such as the –

(i) recipient or category of recipients of the personal data;

(ii) nature or category of the personal data;

(iii) existence of the right of access to and the right to rectify the personal data collected;

(iv) existence of the right to object to the processing of the personal data as referred to in section 20(3); and

(v) right to lodge a complaint to the Authority and the contact details of the Authority,

which is necessary, having regard to the specific circumstances in which the personal data is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

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

(a) if the personal data is collected directly from the data subject, before the personal data is collected, unless the data subject is already aware of the personal data referred to in that subsection; and

(b) in any other case, before the personal data is collected or as soon as reasonably practicable after it has been collected.

(3) A controller or a person acting under the authority of the controller that has previously taken the steps referred to in subsection (1) complies with subsection (1) in relation to the subsequent collection from the data subject of the same personal data or personal data of the same kind if the purpose of collection of the personal data remains the same.

(4) It is not necessary for a controller or a person acting under the authority of the controller to comply with subsection (1) if –

(a) the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;

(b) non-compliance would not prejudice the legitimate interests of the data subject set out in this Act;

(c) non-compliance is necessary –

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of Namibia Revenue Agency Act, 2017 (Act No. 12 of 2017);

(iii) for the conduct of proceedings in any court or tribunal that has commenced or is reasonably contemplated; or

(iv) in the interests of national security.

(d) compliance would prejudice a lawful purpose of the collection;

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

(f) the information will –

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

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

27. Security measures on integrity and confidentiality of personal data

(1) A controller must secure the integrity and confidentiality of personal data in his or her possession or under his or her control by taking appropriate, reasonable technical and organisational measures to prevent -

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

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

(2) In order to give effect to subsection (1), a controller must take reasonable measures to –

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

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

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

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

(3) A controller must have due regard to generally accepted data security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

28. Personal data processed by a data processor or third party

A data processor or third party who process personal data on behalf of a controller or a processor, must -

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

(b) treat personal data which comes to his or her knowledge as confidential and must not disclose it,

unless required by law or in the course of the proper performance of their duties.

29. Security measures regarding information processed by data processor or third party

(1) A controller must, in terms of a written contract between the controller and the data processor or third party, ensure that the data processor or third party which processes personal data for the controller establishes and maintains the security measures referred to in section 27.

(2) The data processor or third party must notify the data controller or a data processor in the case of a third party who processes personal data on behalf of a data processor immediately where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by any unauthorised person.

30. Notification of security compromises

(1) Where there are reasonable grounds to believe that the personal data of a data subject has been accessed or acquired by any unauthorised person, the controller must notify -

(a) the Authority; and

(b) subject to subsection (3), the data subject, unless the identity of the data subject cannot be established.

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

(3) A controller may only delay notification to the data subject if a public body responsible for the prevention, detection or investigation of offences or the Authority determines that the notification will impede a criminal investigation by the public body concerned.

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

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

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

(c) placed in a prominent position on the website of the controller;

(d) published in the news media; and

(e) as may be directed by the Authority.

(5) The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including –

(a) a description of the possible consequences of the security compromise;

(b) a description of the measures that the controller intends to take or has taken to address the security compromise;

(c) a recommendation with regard to the measures to be taken by a data subject to mitigate the possible adverse effects of the security compromise; and

(d) if known to the controller, the identity of the unauthorised person who may have accessed or acquired the personal data.

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

31. Access to personal data

(1) A data subject, having provided adequate proof of identity, has the right to -

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

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

(i) within a reasonable time;

(ii) at a prescribed fee, if any;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

(2) If, in response to a request in terms of subsection (1), personal data is communicated to a data subject, the data subject must be advised of the right in terms of section 32 to request the correction of the personal data.

(3) If a data subject is required by a controller to pay a fee for the services provided to a data subject in terms of subsection (1)(b) to enable the controller to respond to a request, the controller –

(a) must give the applicant a written estimate of the fee before providing the services; and

(b) may require the applicant to pay a deposit for all or part of the fee.

32. Correction of personal data

(1) A data subject may, in the prescribed manner, request a controller to -

(a) correct or delete personal data about the data subject in his or her possession or under his or her control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; and

(b) destroy or delete a record of personal data of a data subject that the controller is no longer authorised to retain in terms of section 23.

(2) On receipt of a request in terms of subsection (1) a controller must, as soon as reasonably practical –

(a) correct the personal data;

(b) destroy or delete the personal data;

(c) provide the data subject, to his or her satisfaction, with credible evidence in support of the personal data; or

(d) where agreement cannot be reached between the controller and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the personal data in such a manner that it will always be read with the personal data, an indication that a correction of the personal data has been requested but has not been made.

(3) If the controller has taken steps under subsection (2) that result in a change to the personal data and the changed personal data has an impact on decisions that have been or will be taken in respect of the data subject in question, the controller must, if reasonably practicable, inform the processor or third party to whom the personal data has been disclosed of those steps.

(4) The controller must notify a data subject who has made a request in terms of subsection (1) of the action taken as a result of the request.

33. Prohibition on processing of special category personal data

(1) A controller may, subject to section 34, not process personal data concerning -

(a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric data of a data subject; or

(b) the criminal behaviour of a data subject to the extent that such data relates to –

(i) the alleged commission by a data subject of any offence; or

(ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

34. General authorisation concerning processing of special personal data

(1) Despite section 33, a controller or a person acting under the authority of a controller may process special categories of personal data if the -

(a) processing is carried out with the consent of a data subject referred to in section 33;

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

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

(d) processing is for historical, statistical or research purposes to the extent that -

(i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or

(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;

(e) personal data has deliberately been made public by the data subject; and

(f) the processing is necessary for:

(i) preventive medicine or medical diagnosis;

(ii) the provision of care or treatment to the data subject; or

(iii) the assessment of the working capacity of an employee; or

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

(v) the management of health or social care systems and services provided in the interest of the data subject; or

(vi) when the data is processed under a contract with a health professional; or

(g) the processing is necessary for reasons of substantial public interest in the area of public health, such as monitoring and protecting against a life-threatening epidemic and its spread, subject to specific measures to safeguard the rights and freedoms of data subjects.

(2) A controller, processor or third party who obtains personal data in contravention of this section commits an offence and is liable to pay a fine to the Authority as prescribed.

35. Authorisation concerning religious or philosophical beliefs of a data subject

(1) The prohibition on processing of personal data of a data subject concerning his or her religious or philosophical beliefs, as referred to in section 33, does not apply if the processing is carried out by -

(a) spiritual or religious organisations, or independent sections of those organisations if –

(i) the information concerns data subjects belonging to those organisations; or

(ii) it is necessary to achieve their aims and principles;

(b) institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; and

(c) other institutions: Provided that the processing is necessary to protect the spiritual welfare of the data subject, unless he or she has indicated that he or she objects to the processing.

(2) In the cases referred to in subsection (1)(a), the prohibition does not apply to processing of personal data concerning the religion or philosophy of life of family members of the data subject if –

(a) the association concerned maintains regular contacts with those family members in connection with its aims; and

(b) the family members have not objected in writing to the processing.

(3) In the cases referred to in subsections (1) and (2), personal data concerning religious or philosophical beliefs of a data subject may not be supplied to third parties without the consent of the data subject.

36. Authorisation concerning race or ethnic origin

The prohibition on processing of personal data concerning race or ethnic origin of a data subject, as referred to in section 33, does not apply if the processing is carried out to –

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

(b) comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

37. Authorisation concerning trade union membership of a data subject

(1) The prohibition on processing of information concerning trade union membership of a data subject, as referred to section 33, does not apply to the processing by a trade union to which the data subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union or trade union federation.

(2) In the cases referred to in subsection (1), no personal data may be supplied to third parties without the consent of the data subject.

38. Authorisation concerning political persuasion of a data subject

(1) The prohibition on processing of personal data concerning political persuasion of a data subject, as referred to in section 33, does not apply to processing by or for an institution, founded on political principles, of the personal data of -

(a) its members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institution; or

(b) a data subject if such processing is necessary for the purposes of –

(i) forming a political party;

(ii) participating in the activities of, or engaging in the recruitment of members for canvassing supporters or voters for, a political party with the view to –

(aa) an election of the National Assembly and National Council as regulated in terms of the Electoral Act, 2014 (Act No. 5 of 2014); and

(bb) council elections as regulated in terms of the Local Authorities Act, 1992 and the Regional Councils Act, 1992; or

(iii) campaigning for a political party or cause.

(2) In the cases referred to under subsection (1), no personal data may be supplied to third parties without the consent of the data subject.

39. Authorisation concerning health or sex life of a data subject

(1) The prohibition on processing of personal data concerning health or sex life of a data subject, as referred to section 33, does not apply to the processing by -

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

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

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

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

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

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

(d) any public or private body managing the care of a child if such processing is necessary for the performance of their lawful duties;

(e) any public body, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or

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

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

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

(2) In the cases referred to in subsection (1), the personal data may only be processed by controllers subject to an obligation or confidentiality by virtue of office, profession or legal provision, or established by written agreement between the controller and the data subject.

(3) A controller that is permitted to process personal data concerning the health and sex life of a data subject in terms of this section and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, must treat the personal data as confidential, unless the controller is required by law or in connection with their duties to communicate the personal data to other parties who are authorised to process such personal data in accordance with subsection (1).

(4) The prohibition on processing any of the categories of personal data referred to in section 33, does not apply if it is necessary to supplement the processing of personal data concerning the health of a data subject, as referred to in subsection (1)(a), with a view to the proper treatment or care of the data subject.

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

(a) a serious medical interest prevails; or

(b) the processing is necessary for historical, statistical or research activity.

(6) More detailed rules may be prescribed concerning the application of subsections (1)(b) and (f).

40. Authorisation concerning criminal behaviour or biometric data of a data subject

(1) The prohibition on processing personal data concerning criminal behaviour or biometric data of a data subject, as referred to in section 33, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by controllers who have obtained that personal data

(2) The processing of personal data concerning personnel in the service of the controller must take place in accordance with the rules established in compliance with labour legislation.

(3) The prohibition on processing any of the categories of personal data referred to in section 33 does not apply if such processing is necessary to supplement the processing of personal data on criminal behaviour or biometric data permitted by this section.

41. Prohibition on processing personal data of children

A controller may, subject to section 42, not process personal data concerning a child.

42. General authorisation concerning personal data of a child

(1) The prohibition on processing of personal data of children, as referred to section 41, does not apply if -

(a) carried out with the prior consent of a competent person;

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

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

(d) for historical, statistical or research purposes to the extent that –

(i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or

(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or

(e) of personal data which has deliberately been made public by the child with the consent of a competent person.

(2) The Authority may, despite the prohibition referred to in section 34, but subject to subsection (3), upon application by a controller and by notice in the Gazette, authorise a controller to process the personal data of a child if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal data of the child.

(3) The Authority may impose reasonable conditions in respect of any authorisation granted under subsection (2), including conditions with regard to how a controller must –

(a) upon request of a competent person provide a reasonable means for that person to –

(i) review the personal data processed; and

(ii) refuse to permit its further processing;

(b) provide notice –

(i) regarding the nature of the personal data of a child that is processed;

(ii) how such personal data is processed; and

(iii) regarding any further processing practices;

(c) refrain from any action that is intended to encourage or persuade a child to disclose more personal data about himself or herself than is reasonably necessary given the purpose for which it is intended; and

(d) establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

PART 4

EXCEPTIONS

43. Exceptions

(1) A prescribed exception must pursue a legitimate purpose and be a necessary and proportionate measure for the protection of -

(a) national security;

(b) defence;

(c) public safety;

(d) important economic and financial interests of the State;

(f) the impartiality and independence of the judiciary of Namibia;

(g) the prevention, investigation and prosecution of criminal offences;

(h) the execution of criminal penalties;

(i) other essential objectives of general public interest; or

(j) the protection of the data subject or the rights and fundamental freedoms of others.

(2) The regulation referred to in subsection (1) must contain the following -

(a) the purposes of the processing or the categories of processing;

(b) the categories of personal data;

(c) the scope of the restrictions introduced;

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

(e) a description of the controller or categories of controllers;

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

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

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

(3) The use of exceptions and restrictions must be subject to objective and adequate safeguards to be considered lawful and to guard against their arbitrary application.

(4) No blanket or unnecessary broad exceptions must be defined in legislation.

(5) Any restriction must be documented by the controller and be made available to the Authority on request.

(6) Processing activities carried out for national security and defence purposes must be subject to independent and effective review and supervision.

PART 5

CODES OF CONDUCT

44. Issuing of codes of conduct

(1) The Authority may from time to time issue codes of conduct.

(2) A code of conduct must –

(a) incorporate all the conditions for the lawful processing of personal data or set out obligations that provide a functional equivalent of all the obligations set out in those conditions; and

(b) prescribe how the conditions for the lawful processing of personal data that are to be applied, or are to be complied with, given the particular features of the sector or sectors of society in which the controller operate.

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

(a) any specified personal data or class of personal data;

(b) any specified body or class of bodies;

(c) any specified activity or class of activities; or

(d) any specified industry, profession, or vocation or class of industries, professions or vocations.

(4) A code of conduct must also –

(a) specify appropriate measures –

(i) for personal data matching programmes if such programmes are used within a specific sector; or

(ii) for protecting the legitimate interests of data subjects in so far as automated decision making is concerned;

(c) provide for the review of the code by the Authority; and

(d) provide for the expiry of the code.

45. Process for issuing of codes of conduct

(1) The Authority may issue a code of conduct under section 45 -

(a) on the Authority's own initiative, but after consultation with affected stakeholders or a body representing such stakeholders; or

(b) on the application, in the prescribed form, by a body which is, in the opinion of the Authority, sufficiently representative of any class of bodies, or of any industry, profession or vocation as defined in the code

in respect of such class of bodies or of any such industry, profession or vocation.

(2) The Authority must give notice in the *Gazette* that the issuing of a code of conduct is being considered, which notice must contain a statement that –

(a) the details of the code of conduct being considered, including a draft of the proposed code, may be obtained from the Authority; and

(b) submissions on the proposed code of conduct may be made in writing to the Authority within such period as is specified in the notice.

(3) The Authority may not issue a code of conduct unless it has considered the submissions made to the Authority in terms of subsection (2)(b), if any, and is satisfied that all persons affected by the proposed code have made a reasonable opportunity to be heard.

(4) The decision as to whether an application for the issuing of a code has been successful must be made within a reasonable period which must not exceed 90 days.

46. Notification, availability and commencement of codes of conduct

(1) If a code of conduct is issued under section 44 the Authority must ensure that –

(a) a notice is published in the *Gazette*, as soon as reasonably practicable after the code is issued, indicating –

(i) that the code has been issued; and

(ii) where copies of the code are available for inspection free of charge and for purchase;

(b) as long as the code remains in force, copies of it are available –

(i) on the website of the Authority;

(ii) for inspection by members of the public free of charge at the offices of the Authority; and

(iii) for purchase or copying by members of the public at a reasonable price at the offices of the Authority.

(2) A code of conduct issued under section 44 comes into force on the 28th day after the date of its notification in the Gazette or on such later date as may be specified in the code and is binding on every class or classes of body, industry, profession or vocation referred to therein.

47. Procedure for dealing with complaints

(1) A code of conduct may prescribe procedures for making and dealing with complaints alleging a breach of the code, but no such provision may limit or restrict the enforcement of this Act.

(2) If the code sets out procedures for making and dealing with complaints, the Authority must be satisfied that –

(a) the procedures meet the –

(i) prescribed standards; and

(ii) guidelines issued by the Authority in terms of section 49, relating to the making of and dealing with complaints;

(b) the code provides for the appointment of an independent adjudicator to whom complaints may be made;

(c) the code requires the adjudicator to prepare and submit a report, in a form satisfactory to the Authority within six months of the end of the financial year of the Authority on the operation of the code during that financial year; and

(d) the code requires the report prepared for each year to specify the number and nature of complaints made to an adjudicator under the code during that financial year.

(3) A controller or data subject who is aggrieved by a determination, including any declaration, order or direction that is included in the determination, made by an adjudicator after having investigated a complaint relating to the protection of personal data under an approved code of conduct, may submit a complaint to the Authority against the determination upon payment of a prescribed fee.

(4) The determination by the adjudicator continues to have effect unless and until the Authority makes a determination relating to the complaint made to it or unless the Authority determines otherwise.

48. Amendment and revocation of codes of conduct

(1) The Authority may amend or revoke a code of conduct issued under section 44.

(2) The provisions of sections 44 to 47 apply in respect of any amendment or revocation of a code of conduct.

49. Guidelines about codes of conduct

(1) The Authority may provide written guidelines -

(a) to assist bodies to develop codes of conduct or to apply approved codes of conduct;

(b) relating to making and dealing with complaints under approved codes of conduct; and

(c) about matters the Authority may consider in deciding whether to approve a code of conduct or a variation or revocation of an approved code of conduct.

(2) The Authority must have regard to the guidelines developed by it and the provisions of this Act when considering the approval of a code of conduct for the processing of personal data where the controller is not subject to a code of ethics.

(3) Before providing guidelines for the purposes of subsection (1)(b), the Authority must give everyone the Authority considers has a real and substantial legitimate interest in the matters covered by the proposed guidelines an opportunity to comment on them.

(4) The Authority must publish guidelines provided under subsection (1) in the *Gazette*.

50. Register of approved codes of conduct

(1) The Authority must keep a register of approved codes of conduct.

(2) The Authority may decide the form of the register and how it is to be kept.

(3) The Authority must make the register available to the public in the way that the Authority determines.

(4) The Authority may charge reasonable fees for –

(a) making the register available to the public; or

(b) providing copies of, or extracts from, the register.

51. Review of operation of approved codes of conduct

(1) The Authority may, on its own initiative, review the operation of an approved code of conduct.

(2) The Authority may do one or more of the following for the purposes of the review:

(a) Consider the process under the code for making and dealing with complaints;

(b) inspect the records of an adjudicator for the code;

(c) consider the outcome of complaints dealt with under the code;

(d) interview an adjudicator for the code; and

(e) appoint experts to review those provisions of the code that the Authority believes require expert evaluation.

(3) The review may inform a decision by the Authority under section 48 to revoke the approved code of conduct with immediate effect or at a future date to be determined by the Authority.

52. Effect of failure to comply with code of conduct

If a code of conduct issued under section 44 is in force, failure to comply with the code is deemed to be a breach of the conditions for the lawful processing of personal data referred to in Part 2 and a controller or a person acting under the authority of a controller who unlawfully breach the conditions for lawful processing of personal data in contravention of this section commits an offence and is liable to pay a fine to the Authority as prescribed.

PART 6

TRANSBORDER FLOWS OF PERSONAL DATA

53. Transfer of personal data outside Namibia

(1) A controller in Namibia may not transfer personal data of a data subject to a processor or third party who is in a foreign country unless -

(a) the processor or third party who is the recipient of the personal data is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that –

(i) effectively upholds principles for reasonable processing of personal data that is substantially similar to the conditions for lawful processing of personal data relating to a data subject in Namibia; and

(ii) includes provisions that are substantially similar to this section relating to the further transfer of personal data from the controller to the processor or third party who is in a foreign country;

(b) the data subject consents to the transfer;

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

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

(e) the transfer is for the benefit of the data subject, and –

(i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

(ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

(2) For the purpose of this section –

(a) "binding corporate rules" means personal data processing policies, within a group of undertakings, which are adhered to by a controller or processor within that group of undertakings when transferring personal data to a controller or processor within that same group of undertakings in a foreign country; and

(b) "group of undertakings" means a controlling undertaking and its controlled undertakings.

(3) The Authority must be involved in assessing if any of the criteria are met when using the above-mentioned exceptions.

(4) A controller or a processor must document the assessment of the appropriate safeguards or the criteria referred to under subsection (1) and the Authority must be provided with all relevant information concerning the transfer referred to in subsection (1) to demonstrate the effectiveness of the safeguards or the existence of any of the criteria referred to in subsection (1).

(5) The Authority may prohibit, suspend, or revoke the transfer of personal data to a controller, processor or third party under this section.

PART 7

ENFORCEMENT

54. Interference with the protection of personal data of a data subject

For purposes of this Part 7, interference with the protection of the personal data of a data subject consists, in relation to that data subject, of -

(a) any breach of the conditions for the lawful processing of personal data referred to in Part 3;

(b) non-compliance with the provisions of this Act; or

(c) a breach of the provisions of the code of conduct issued in terms of section 44.

55. Complaints

(1) Any person may submit a complaint to the Authority in the prescribed manner and form alleging interference with the protection of the personal data of a data subject.

(2) A controller or data subject may, in terms of section 46(3), submit a complaint to the Authority in the prescribed manner and form if he or she is aggrieved by the determination of an adjudicator.

56. Mode of complaints to Authority

(1) A complaint to the Authority must be made in writing.

(2) The Authority must give such reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Authority, to put the complaint in writing.

57. Action on receipt of complaint

(1) On receiving a complaint in terms of section 55, the Authority may -

(a) conduct a pre-investigation as referred to in section 60;

(b) act, at any time during the investigation and where appropriate, as conciliator in relation to any interference with the protection of personal data of a data subject in the prescribed manner;

(c) decide, in accordance with section 58, to take no action on the complaint or, as the case may be, require no further action in respect of the complaint;

(d) conduct a full investigation of the complaint;

(e) refer the complaint to a mediator; or

(f) take such further action as is contemplated by this Part 7.

(2) The Authority must, as soon as is reasonably practicable, advice the complainant and the controller to whom the complaint relates of the course of action that the Authority proposes to adopt under subsection (1).

(3) The Authority may, on its own initiative, commence an investigation into the interference with the protection of the personal data of a data subject as referred to in section 54.

58. Authority may decide to take no action on complaint

(1) The Authority, after investigating a complaint received in terms of section 54, may decide to take no action or, as the case may be, require no further action in respect of the complaint if, in the Authority's opinion -

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

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

(c) the complaint is frivolous or vexatious or is not made in good faith;

(d) the complainant does not desire that action be taken or, as the case may be, continued;

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

(f) in cases where the complaint relates to a matter in respect of which a code of conduct is in force and the code of conduct makes provision for a complaints procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.

(2) Despite subsection (1), the Authority may in its own discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Authority that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

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

59. Referral of complaint to regulatory body

(1) If, on receiving a complaint in terms of section 55, the Authority considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body established in terms of any law, the Authority must forthwith determine whether the complaint should be dealt with, in whole or in part, under this Act after consultation with the body concerned.

(2) If the Authority determines that the complaint should be dealt with by another body, the Authority must forthwith refer the complaint to that body to be dealt with accordingly and must notify the complainant of the referral.

60. Pre-investigation proceedings of Authority

Before proceeding to investigate any matter in terms of this Part 7, the Authority must, in the prescribed manner, inform –

(a) the complainant, the data subject to whom the investigation relates (if not the complainant) and any person alleged to be aggrieved (if not the complainant), of the Authority's intention to conduct the investigation; and

(b) the controller to whom the investigation relates of the –

(i) details of the complaint or, as the case may be, the subject matter of the investigation; and

(ii) right of that controller to submit to the Authority, within a reasonable period, a written response in relation to the complaint or, as the case may be, the subject matter of the complaint.

61. Settlement of complaints

If it appears from a complaint, or any written response made in relation to a complaint under section 60(b)(ii), that it may be possible to secure –

(a) a settlement between any of the parties concerned; and

(b) if appropriate, a satisfactory assurance against the repetition of any action that is the subject matter of the complaint or the doing of further actions of a similar kind by the person concerned,

the Authority may, without investigating the complaint or, as the case may be, investigating the complaint further, in the prescribed manner, use its best endeavours to secure such a settlement and assurance.

62. Investigation proceedings of Authority

For the purposes of investigation of a complaint the Authority may –

(a) summon and enforce the appearance of persons before the Authority and compel them to give oral or written evidence on oath and to produce any records and things that the Authority considers necessary to investigate the complaint, in the same manner and to the same extent as the High Court;

(b) administer oath;

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

(d) at any reasonable time, subject to this section, enter and search any premises occupied by a controller;

(e) conduct a private interview with any person in any premises entered under section 65 subject to section 62; and

(f) otherwise carry out in those premises any inquiries that the Authority sees fit in terms of section 62.

63. Issue of warrants

(1) A judge of the High Court, a regional magistrate or a magistrate, if satisfied by information on oath supplied by the Authority that there are reasonable grounds for suspecting that -

(a) a controller is interfering with the protection of personal data of a data subject; or

(b) an offence under this Act has been or is being committed,

and that evidence of the contravention or of the commission of the offence is to be found on any premises specified in the information, that are within the jurisdiction of that judge or magistrate, may, subject to subsection (2), grant a warrant to enter and search such premises.

(2) A warrant issued under subsection (1) authorises any of the Authority's members or staff members, subject to section 65, at any time within seven days of the date of the warrant to enter the premises as identified in the warrant, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data and to inspect and seize any record, other material or equipment found there which may be such evidence as is mentioned in that subsection.

64. Requirements for issuing of warrants

(1) A judge or magistrate must not issue a warrant under section 63 unless satisfied that -

(a) the Authority has given seven days' notice in writing to the occupier of the premises in question demanding access to the premises;

(b) either –

(i) access was demanded at a reasonable hour and was unreasonably refused; or

(ii) although entry to the premises was granted, the occupier was unreasonably refused to comply with a request by any of the members or members of staff of the Authority to permit the members or members of staff to do any of the things referred to in section 63(2); and

(c) that the occupier, has, after the refusal, been notified by the Authority of the application for the warrant and has had an opportunity of being heard on the question whether the warrant should be issued.

(2) Subsection (1) does not apply if the judge or magistrate is satisfied that the case is one of urgency or that compliance with that subsection would defeat the object of the entry.

(3) A judge or magistrate who issues a warrant under section 63 must also issue two copies of it and certify them clearly as copies.

65. Execution of warrants

(1) A police officer who is assisting a person authorised to conduct an entry and search in terms of a warrant issued under section 63 may overcome resistance to the entry and search by using such force as is reasonably necessary.

(2) A warrant issued under this section must be executed at a reasonable hour unless it appears to the person executing it that there are reasonable grounds for suspecting that the evidence in question would not be found if it were so executed.

(3) If the person who occupies the premises in respect of which a warrant is issued under section 63 is present when the warrant is executed, he or she must be shown the warrant and be supplied with a copy of it, and if that person is not present a copy of the warrant must be left in a prominent place on the premises.

(4) A person seizing anything in pursuance of a warrant under section 63 must give a receipt to the occupier or leave the receipt on the premises.

(5) Anything so seized may be retained for as long as is necessary in all circumstances but the person in occupation of the premises in question must be given a copy of any documentation that is seized if he or she so requests and the person executing the warrant considers that it can be done without undue delay.

(6) A person authorised to conduct an entry and search in terms of section 63 must be accompanies and assisted by a police officer.

(7) A person who enters and searches any premises under this section must conduct the entry and search with strict regard for decency and order, and with regard to each person's right to dignity, freedom, security and privacy.

(8) A person who enters and searches premises under this section must before questioning any person –

(a) advise that person of the right to be assisted at the time by a legal practitioner; and

(b) allow that person to exercise that right.

(9) No self-incriminating answer given or statement made to a person who conducts a search in terms of a warrant issued under section 63 is admissible as evidence against the person who gave the answer or made the statement in criminal proceedings, except in criminal proceedings for perjury or in which that person is tried for an offence then only to the extent that the answer or statement is relevant to prove the offence charged.

66. Matters exempt from search and seizure

If the Authority has granted an exception in terms of section 41, the personal data that is processed in terms of that exception is not subject to search and seizure empowered by a warrant issued under section 63.

67. Communication between legal adviser and client exempt

(1) Subject to the provisions of this section, the powers of search and seizure conferred by a warrant issued under section 63 must not be exercised in respect of -

(a) any communication between a professional legal adviser and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights; or

(b) any communication between professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act, including proceedings before a court, and for the purposes of such proceedings.

(2) Subsection (1) applies also to –

(a) any copy or other record of any such communication as is mentioned therein; and

(b) any document or article enclosed with or referred to in any such communication if made in connection with the giving of any advice, as the case may be, in connection with or in contemplation of and for the purposes of such proceedings as are mentioned therein.

68. Objection to search and seizure

If the person in occupation of any premises in respect of which a warrant is issued under this Act objects to the inspection or seizure under the warrant of any material on the ground that it –

(a) contains privileged information and refuses the inspection or removal of such article or document, the person executing the warrant or search must, if he or she is of the opinion that the article or document contains information that has a bearing on the investigation and that such information is necessary for the investigation, request the Registrar of the High Court which has jurisdiction or his or her delegate, to attach and remove that article or document for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not; or

(b) consists partly of matters in respect of which those powers are not exercised, he or she must, if the person executing the warrant so

requests, furnish that person with a copy of so much of the material as is not exempt from those powers.

69. Return of warrants

A warrant issued under section 63 must be returned to the court from which it was issued –

(a) after being executed; or

(b) if not executed within the time authorised for its execution,

and the person who has executed the warrant must take an endorsement on it stating what powers have been exercised by him or her under the warrant.

70. Assessment

(1) The Authority, on its own initiative, or at the request by or on behalf of the controller, a data subject or any other person must make an assessment in the prescribed manner of whether an instance of processing of personal data complies with the provisions of this Act.

(2) The Authority must make the assessment if it appears to be appropriate, unless, where the assessment is made on request, the Authority has not been supplied with such information as it may reasonably require in order to –

(a) satisfy itself as to the identity of the person making the request; and

(b) enable it to identify the action in question.

(3) The matters to which the Authority may have regard in determining whether it is appropriate to make an assessment include –

(a) the extent to which the request appears to it to raise a matter of substance'

(b) any undue delay in making the request; and

(c) whether or not the person making the request is entitled to make an application in terms of section 31 or 32 in respect of the personal data in question.

(4) If the Authority has received a request under this section it must notify the requester –

(a) whether it has made an assessment as a result of the request; and

(b) to the extent that it considers appropriate, having regard in particular to any exemption which has been granted by the Authority in terms of section 43 from section 31 or 32 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request.

71. Parties to be informed of assessment

(1) After completing the assessment referred to in section 70 the Authority -

(a) must report to the controller the results of the assessment and any recommendations that the Authority considers appropriate; and

(b) may, in appropriate cases, require the controller, within a specified time, to inform the Authority of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(2) The Authority may make public any information relating to the personal data management practices of a controller that has been the subject of an assessment under this section if the Authority considers it in the public interest to do so.

(3) A report made by the Authority under subsection (1) is deemed to be the equivalent of an enforcement notice.

PART 8

GENERAL PROVISIONS

72. Fees

(1) The Minister may, subject to section 74 and after consultation with the Authority, prescribe fees to be paid by data subjects -

(a) to a controller; and

(b) to the Authority.

(2) Different fees may be prescribed in respect of different categories of controllers and data subjects referred to in subsection (1).

73. Regulations

(1) The Minister may, subject to section 74, make regulations relating to -

(a) the establishment of the Authority; and

(b) fees referred to in section 72(1).

(2) The Authority may, subject to section 74, make regulations relating to –

(a) the manner in which a data subject may object to the processing of personal data referred to in section 20;

(b) the manner in which a data subject may submit a request to a controller in terms of section 32(1);

(c) the processing of personal data by a controller relating to health in terms of section 39;

(d) the form in terms of which an application for a code of conduct must be submitted to the Authority as referred to in terms of section 41(1)(b);

(e) the manner and form within which the consent of the data subject must be requested;

(f) the manner and form in terms of which a complaint must be submitted in terms of section 55;

(g) the Authority acting as conciliator in relation to any interference with the protection of personal data as referred to in section 57(1)(b);

(h) the notification of the parties concerned of the investigation to be conducted as referred to section 60.

(i) the settlement of complaints as referred to in section 61;

(j) the manner in which an assessment of the processing of personal data will be made as referred to in section 70(1);

(k) the manner in terms of which the parties concerned must be informed of the developments during and result of an investigation; and

(l) matters incidental to the imposition of administrative fines .

74. Procedure for making regulations

(1) The Minister, before making or amending any regulations referred to in section 73(1), must publish a notice in the *Gazette* -

(a) setting out that draft regulations have been developed;

(b) specifying where a copy of the draft regulations may be obtained; and

(c) inviting written comments to be submitted on the proposed regulations within a specified period.

(2) After complying with subsection (1) and after consultation with the Authority in respect of the draft regulations referred to in section 73, the Minister may –

(a) amend the draft regulations; and

(b) subject to subsection (5), publish the regulations in the final form in the *Gazette*.

(3) The Authority, before making or amending any regulations referred to in section 73(2), must publish a notice in the Gazette –

(a) setting out that the draft regulations have been developed;

(b) specifying where a copy of the draft regulations may be obtained; and

(c) inviting written comments to be submitted on the proposed regulations within a specified period.

(4) After complying with subsection (3), the Authority may –

(a) amend the draft regulations; and

(b) subject to subsection (5), publish the regulations in final form in the *Gazette*.

(5) (a) The Minister or the Authority, as the case may be, must, within 30 days before publication of the regulations in the Gazette, as referred to in subsection (2)(b) or (4)(b), table them in Parliament.

(b) Subsection (1) or (3) does not apply in respect of any amendment of the regulations as a result of the process referred to in paragraph (a).

75. Transitional arrangements

(1) All processing of personal data of data subjects must within one year after the commencement of this section be made to conform to this Act.

(2) The period of one year referred to in subsection (1) may be extended by the Minister, on request or of his or her own accord and after consultation with the Authority, by notice in the *Gazette* in respect of different class or classes of personal data and bodies by an additional period which period may not exceed three years.

76. Short title and commencement

(1) This Act is called the Data Protection Act, 2021, and comes into operation on a date determined the Minister by notice in the *Gazette*.

(2) Different dates of commencement may be determined in respect of different provisions of this Act or in respect of different class or classes of personal data and bodies.