Act…

DRAFT DATA PROTECTION BILL

The purpose of this ACT is 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 establish obligations of data controllers and processors; to establish a Data Protection Authority and to provide for its functions; to provide for restrictions and exceptions under the provisions of this Act and for matters connected therewith.

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

ARRANGEMENT OF SECTIONS

PART V
OBLIGATIONS OF CONTROLLERS AND PROCESSORS

PART VI
TRANSBORDER FLOWS OF PERSONAL DATA

PART VII
DATA PROTECTION SUPERVISORY AUTHORITY

~~**PART VII**~~
~~**RECOURSE TO THE JUDICIAL AUTHORITY**~~

Formatted: Left, Indent: Left: 0 cm, First line: 0 cm

Formatted: Left

Formatted: Left, Indent: Left: 0 cm, First line: 0 cm

Formatted: Indent: Left: 0 cm, First line: 0 cm

Formatted: Left, Indent: Left: 0 cm, First line: 0 cm, Don't keep with next, Don't keep lines together

PART VIII
OFFENCES AND PENALTIES

~~40~~38. Specific Offences
~~41~~39. Penalties

Formatted: Indent: Left: 0 cm, Hanging: 1,27 cm, Tab stops: Not at 4,55 cm

Formatted: Indent: Left: 0 cm, Hanging: 1,27 cm, Tab stops: Not at 4,55 cm

~~**PART X**~~
~~**REPEAL OF LAWS AND SHORT TITLE**~~

~~43. Short title and commencement~~
~~44. Repeal of laws~~

PART 1
PRELIMINARY

1. Definitions

For purposes of this Act:

"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 or 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) To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify the said person.

(c) An individual 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 or set of operations performed on personal data, whether or not it occurs by automatic mean, and includes, but not exhaustively, 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;

Where automated processing is not used, 'processing' means an operation or set of operations performed upon personal data within a structured set of such data, which are accessible or retrievable according to specific criteria allowing the controller or any other person to search, combine or correlate the data to a specific data subject;

"processor" means a natural or legal person which processes personal data on behalf of the controller. Instructions that a controller is required to provide to a processor shall limit what the processor is permitted to do with the personal data;

"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 natural or legal person or public body to whom data are disclosed or made available;

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

"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. The processing of such data shall be prohibited or allowed only subject to appropriate safeguards under PART II Section 7 of this Act;

"third party" means any natural or legal person, organization or public authority 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. 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 individuals with regard to the processing of personal data whatever his or her nationality or residence and in particular by;

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

(b) conferring on individuals several rights as set out in **PART III** including the right to access and to know the underlying reasoning of the processing, and the right to the rectification and erasure of their personal data, and the right to remedy.

(3) This Act applies to the processing of personal data carried out by controllers, and where applicable processors, in the private and public sectors.

(4) This Act applies to the processing of personal data undertaken within the territory of Namibia as well as to the processing of personal data undertaken 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 II

BASIC PRINCIPLES AND LAWFUL PROCESSING

3. Basic Principles relating to the processing of Personal Data

(1) Fair, transparent and lawful processing

(a) Personal data must be processed fairly.

(b) Personal data must be processed transparently. Data subjects have the right to know about the processing of their personal data in accordance with Section 8 of this Act.

(c) Personal data must be processed lawfully.

(2) Specific Legitimate Purpose and Purpose Limitation

(a) Personal data must be processed for explicit, specified and legitimate purposes and any further processing must not be incompatible with those specified purposes.

(b) Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes may be considered compatible with those purposes, subject to appropriate safeguards.

(3) Data Minimisation

(a) Personal data undergoing processing must be adequate, relevant and not excessive in relation to the purposes for which they are processed. This requirement shall not only refer to the quantity but also the quality of personal data.

(4) Accuracy

(a) Personal data undergoing processing shall be accurate and, to the extent necessary, must be kept up to date.

(5) Storage Limitation

(a) Personal data undergoing processing shall be preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

(b) Personal data must be deleted once the purpose for which it was processed has been achieved or must only be kept in a form that prevents any direct or indirect identification of the data subject.

4. Lawfulness of processing

(1) The processing of personal data shall be proportionate and appropriate in relation to the purpose or purposes pursued, taking into account the interests, rights and freedoms of data subjects, and shall be considered lawful only if it meets at least one of the following bases:

(a) the data subject gives his or her consent to a specified purpose, subject to the conditions of consent set out in Section 5;

(b) the processing is necessary for entering into or for the fulfilment of a contract to which the data subject is a party;

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

(d) the processing is necessary to protect the vital interests of the data subject or another person;

(e) the processing is necessary for the legitimate interests of the controller or a third party, except where such interests may prejudice or harm the interests, rights and freedoms of data subjects and that override those of the controller or third-party;

(f) 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; or

(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.

(2) Paragraph (e) of subsection (1) does not apply to the processing of personal data by public authorities in the performance of their tasks established under any other law.

(3) Where the processing is carried out for a purpose which is not the original purpose for which the personal data were 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 subjects;

(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 protections afforded, such as special categories of personal data or data related to criminal offences and convictions;

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

5. Conditions for Consent

(1) Where the processing of personal data is based on the consent of a data subject, the controller must be able to demonstrate evidence of such consent.

(2) Consent must be a freely given, specific, informed and unambiguous affirmative action, given either by electronic means or a written or oral statement, by which the data subject clearly indicates his or her acceptance of the proposed processing of his or her personal data.

(3) A request for consent must be presented in a manner that is clearly distinguishable from other matters, and that is intelligible using clear and plain language.

(4) Consent should cover all processing activities carried out for the same purpose or purposes. In the case of multiple purposes, consent should be given for each individual and specific purpose, where consent is the only lawful basis relied upon.

(5) A data subject has the right to withdraw any consent given, at any time and free of charge. It must be as easy to withdraw consent as it is to give consent. Before giving consent, the data subject must be informed of their right to withdraw consent and how they may do so.

(6) The withdrawal of consent shall not affect the lawfulness of the data processing that occurred before the data controller received the withdrawal of consent but must not allow for the continued processing of data, unless processing is based on some other legitimate basis laid down by law.

(7) No undue influence or pressure, of an economic or other nature, whether direct or indirect, may be exercised on the data subject and consent shall not be regarded as freely given where the data subject has no genuine or free choice or is unable to refuse or withdraw consent without prejudice.

6. Personal data of a child

(1) Where a child is below the age of 18, the processing of their personal data shall be lawful where:

(a) it is based on the consent given by the child's parent or legal guardian unless the law states that the child may act by himself or herself without being represented by his or her parents or legal guardian;

(b) it is in the vital interests of the child;

(c) it is necessary to meet a legal obligation to which the controller is subject; or

(d) it is necessary for the performance of a task carried out by the controller and that is in the public interest.

(2) Where the personal data of a child below the age of 18 years are involved, and the processing is based on consent, a controller shall make every reasonable effort to verify that consent has been given or authorised, taking into account available technology.

7. Processing of Special Categories of Personal Data

(1) The processing of special categories of 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, may entail risks to data subjects independently of the context of the processing, and is prohibited

unless, additional safeguards, complementing those provided for by the Act have been put in place, and that shall include:

(a) the data subject has given his or her explicit consent to the specified purpose or purposes subject to the conditions set out in Section 5 except where the law provides that the prohibition cannot be lifted even with the written consent of the data subject;

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

(c) the processing necessary for carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security and social protection law;

(d) the processing carried out in the course of the controller's legitimate activities, with appropriate safeguards, by a foundation, association or any other non-profit body with a political, philosophical, religious, health-insurance or trade-union purpose and on condition that the processing relates solely to the members of the organization or to persons who have regular contact with it in connection with such purposes and that the data is not disclosed to a third party without the data subjects' consent;

(e) the processing necessary for preventive medicine or medical diagnosis, the provision of care or treatment to the data subject, or the assessment of the working capacity of an employee, or the provision of health or social care or treatment or the management of health or social care systems and services provided in the interest of the data subject, or when the data is processed under a contract with a health professional and subject to appropriate safeguards; or

(f) the processing 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) Special categories of personal data referred to in subsection (1) may be processed for the purposes set out in paragraph (f) of subsection (1) when the data are processed under the responsibility of a professional subject to a duty of secrecy.

PART III

RIGHTS OF THE DATA SUBJECT

8. Right to know and access

(1) Data subjects shall have the right to obtain, on request and at reasonable intervals:

(a) confirmation as to whether or not personal data about them are being processed and if so, to receive the following information:

(i) the identity of the controller;

(ii) the purposes of the processing;

(iii) the source of the personal data undergoing processing;

(iv) the recipients or categories of recipients that the personal data are disclosed to;

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

(vi) any other information that the controller is required to provide to ensure the transparency of processing in accordance with Section 16;

(vii) where requested, a copy of the personal data undergoing processing

(2) The controller shall provide a copy of the personal data undergoing processing free of charge and in an intelligible form. In exceptional circumstances a controller may charge a reasonable fee based on the administrative costs incurred where a request is excessive or manifestly unfounded, in particular because of their repetitive character.

(3) The controller shall provide a copy of the personal data requested together with the information under paragraph 1 without delay and in any event within one month after the date of receipt of a request. That period may be extended by a further period of one month, where necessary, taking into account the complexity of the request. A controller shall explain the reasons for any delay in meeting a request under this section.

(4) Data subjects have the right, on request, to obtain knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her, including the consequences of such reasoning.

9. Right to rectification, erasure, and restriction of processing

(1) The data subject has the right to obtain from the controller, without excessive delay and free of charge, the rectification of inaccurate, incomplete, or unlawfully processed personal data.

(2) A data subject has the right to have incomplete personal data completed by the recording of a supplementary statement.

(3) The data subject has the right to obtain from the controller, without excessive delay and free of charge, the erasure of personal data where one of the following conditions applies:

(a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws his or her consent on which the processing is based and there are no other legitimate grounds for processing the personal data;

(c) the data subject objects to the processing and the controller cannot demonstrate overriding legitimate grounds for the processing in accordance with this Act;

(d) the processing is unlawful; or

(e) the personal data must be erased to comply with a legal obligation to which the controller is subject.

(4) A data subject has the right to obtain from the controller the restriction of the processing of personal data, for a period necessary, where:

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

(b) the controller no longer needs the personal data, but the data subject requires the personal data for the establishment, exercise or defence of a legal claim;

(c) the data subject objects to the processing of his or her personal data processed on the basis of point (e) or (f) of Section 4(1) of this Act, pending justification by the controller that the legitimate interests of the controller override those of the data subject.

(5) Where the data subject has submitted a valid request for the rectification, erasure or restriction of his or her personal data pursuant to subsection (1) (2) and (3) of this section, the controller must communicate such request to all recipients of the personal data to ensure complete rectification, erasure or restriction, unless the controller can demonstrate this shall prove to be impossible or will involve disproportionate effort on the part of the controller.

10. Right to object

(1) A data subject has the right at any time and free of charge, to object on grounds relating to his or her situation, to the processing of his or her personal data unless the controller demonstrates legitimate grounds for the processing which overrides the interests or rights and fundamental freedoms of the data subject.

(2) A data subject has the right to object, at any time and free of charge, to the processing of his or her personal data for the purposes of direct marketing, including profiling, to the extent that it is related to such processing.

(3) Where a data subject objects to the processing of personal data for the purpose of direct marketing, the personal data shall no longer be processed for that purpose.

(4) Where personal data is processed to communicate direct marketing via electronic means, this shall require the prior consent of the data subject according to the conditions laid down in Section 5.

11. Right not to be subject to automated decision making, including profiling

(1) A data subject has the right not to be subject to a decision significantly affecting him or her based solely on the automated processing of his or her personal data without having his or her views taken into consideration.

(2) Subsection (1) shall not apply if a decision:

(a) is authorised by law to which the controller is subject and which provides appropriate measures to safeguard the legitimate interests, rights and freedoms of data subjects;

(b) necessary for entering into or for the performance of a contract between the data subject and the controller;

(c) is based on the data subject's consent.

(3) Where paragraphs (a) and (c) of subsection (2) apply, the data controller must implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller and to put forward his or her point of view and to challenge the decision.

(4) Where a decision under paragraph 2 is based on special categories of personal data according to Section 7(1) the processing shall only be carried out if conditions for the processing as set out in Section 7 are met and the processing is set forth by law and is necessary for reasons of substantial public interest.

12. Right to obtain assistance from a supervisory authority

The data subject has the right to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Section 25, in exercising his or her rights under this Act.

13. Representation of the data subject

(1) A data subject has the right to mandate a not-for-profit body, organisation or association which has been properly constituted under Namibian law, and that is active in the field of the protection of fundamental rights and freedoms, to:

(a) lodge a complaint on behalf of the data subject, with the Data Protection Supervisory Authority; or

(b) pursue an effective judicial remedy on behalf of the data subject, against a legally binding decision of the Data Protection Supervisory Authority; or

(c) pursue an effective judicial remedy on behalf of the data subject, against a data controller or processor.

(2) Independently of a data subject's mandate, an organisation referred to in subsection (1) has the right to lodge a complaint with the Data Protection Supervisory Authority if it considers the rights of data subjects under this Act have been infringed, if it considers the rights of data subjects under this Act have been infringed systematically or if it involves the rights and freedoms of a large scale of individuals.

14. Right to compensation

(1) Any data subject who has suffered material or non-material damage as a result of an infringement of this Act shall have the right to receive compensation from the controller or processor for the damage suffered.

(2) A controller involved in processing in terms of subsection (1) is liable for the damage caused by processing which infringes this Act. A processor is liable for the damage caused by the processing where it has not complied with obligations of this Act specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(3) A controller or processor is exempt from liability under subsection (2) if it proves that it is not in any way responsible for the event giving rise to the damage.

PART IV

EXCEPTIONS

15. Exceptions

(1) No exception to the provisions set out in this Act shall be allowed except to the provisions of Section 3 [basic principles, except 3(1)(c)], Section 8 [data breach notification], Section 16 [transparency of processing] and Part III [rights of the data subject] when such an exception is provided for by law and pursues a legitimate purpose, respects fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for the protection of:

Commented [TQ1]: This provisions [3(1)(c)]refers to the lawfulness of processing, which under Convention 108+ cannot be subject to exceptions.

(a) national security;

(b) defence,

(c) public safety;

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

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

(f) the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest; or

(g) the protection of the data subject or the rights and fundamental freedoms of others, notably the freedom of expression.

(2) The legislative measure referred to in subsection (1) shall contain specific provisions at least as to:

(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 shall 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 shall be defined in a law.

(5) Any restriction shall be documented by the controller and be made available to the Data Protection Supervisory Authority on request.

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

PART V

OBLIGATIONS OF CONTROLLERS AND PROCESSORS

16. Transparency

(1) Controllers shall act transparently to ensure the fairness of processing and shall inform data subjects in an appropriate manner of key information relating to the processing of their personal data and about their rights.

(2) Controllers shall provide the data subject with minimum information when obtaining personal data either directly or indirectly. Such information must include:

(a) the controller's identity and the contact details of his or her habitual residence or establishment;

(b) the legal basis and the purposes of the intended processing;

(c) the categories of personal data processed;

(d) the recipients or categories of recipients of the personal data, if any; and

(e) the means of exercising the rights set out in Part III.

(3) Such information must be provided in a manner that is clear and easily accessible, using plain language.

(4) Subsection (2) shall not apply where the data subject already has the relevant information.

(5) Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or if it proves to be impossible or involves disproportionate efforts.

17. Data Protection and Privacy by Design and by Default

(1) Before carrying out the processing of personal data, controllers and, where applicable, processors, shall examine its potential impact on the rights and fundamental freedoms of data subjects, and must design the data processing in a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

(2) Controllers and processors shall implement technical and organisational measures which take into account the implications of the right to the protection of personal data at all stages of the data processing.

(3) This implementation of data protection requirements must be achieved not only as regards the technology used for processing the personal data, but also the related work and management policies and processes.

(4) When setting up the technical requirements for default settings, controllers and processors must choose privacy-friendly standard configurations so that the usage of applications and software does not infringe the rights of the data subjects (data protection by

default), and to avoid processing of more personal data than necessary to achieve the legitimate purpose.

18. Security of Processing

(1) To safeguard against risks to the rights and freedoms of data subjects, the controller as well as the processor, must implement appropriate technical and organizational measures to protect personal data and special categories of personal data against accidental or unauthorized access to, use, loss, damage, alteration, disclosure and destruction of the data, transmitted, stored or otherwise processed.

(2) The measures required by subsection (1) must take into account the nature of the personal data and the potential adverse consequences for data subjects, the current state of technological development, and the cost of implementing the measures on the one hand, and the potential risks to the data subject on the other hand and may include:

(a) the pseudonymisation and encryption of personal data;

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

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

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

(3) Controllers and processors must ensure that any person acting under their authority and who has access to personal data shall not process personal data except under the instructions of the controller or processor unless the processing is mandated by law.

(4) Where the processing of personal data is to be carried out by a processor, the controller must:

(a) choose a processor that provides sufficient guarantees to implement security and organisational measures to ensure compliance with this Act and that will ensure the protection of the rights of data subject; and

(b) enter into a written contract with the processor which shall provide that:

(i) the processor shall act only on instructions received from the controller;

(ii) the processor shall not engage another processor except with the prior written authorisation of the controller;

(iii) the processor shall assist the controller in ensuring compliance with its obligations under this Act, including assisting with any audits;

(iv) the categories of personal data to be processed and the purposes of processing are clearly set out; and

(v) the processor shall ensure that any person employed by them is aware of, and complies with, the relevant security measures.

(5) The Data Protection Supervisory Authority may issue guidance on appropriate security measures.

19. Accountability

Controllers and, where applicable, processors, must take all appropriate measures to comply with the provisions set out in this Act and be able to demonstrate that the data processing under their control complies with them.

20. Records of processing activities

(1) Each controller and processor shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

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

(b) the purposes of the processing;

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

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

(e) where possible, the envisaged time limits for erasure of the data;

(f) where possible, a general description of the technical and organisational security measures referred to in Section 18

(2) The records referred to in subsection (1) shall be in writing, including in electronic form.

21. Data Protection Impact Assessment

(1) Controllers and, where applicable, processors, shall examine the likely impact of intended processing operations on the rights and fundamental freedoms of data subjects before the commencement of such processing, and shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

(2) An assessment referred to in subsection (1) shall, in particular, be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling;

(b) processing on a large scale of special categories of personal data; and

(c) systematic monitoring of a publicly accessible area on a large scale.

(3) The assessment shall include at least:

(a) a description of the envisaged processing operations and the purposes of the processing;

(b) an assessment of the necessity and proportionality of the processing operations;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address possible risks, including safeguards, security measures and mechanisms to ensure the protection of personal data.

(4) The Data Protection Supervisory Authority shall establish and publish a list of processing operations that require a data protection impact assessment under this section.

22. Personal data breach notification

(1) The controller must notify the Data Protection Supervisory Authority, without any undue delay, and not later than 72 hours after becoming aware of any personal data breach unless the breach is unlikely to result in a high risk to the rights and freedoms of data subjects.

(2) If a notification is not made within 72 hours the controller must provide reasons for any such delay, and which the Data Protection Supervisory Authority may consider in determining compliance with this Act.

(3) Where a processor becomes aware of a personal data breach, he or she must notify the controller, without undue delay, of any such breach affecting the personal data he or she processes on behalf of the data controller.

(4) The Notification under subsection (1) must at least:

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

(b) the likely consequences of the personal data breach;

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

(5) The controller must document any personal data breach, comprising all facts relating to the personal data breach, its effects and the remedial action taken. That documentation must enable the Data Protection Supervisory Authority to verify compliance with this provision.

(6) The Data Protection Supervisory Authority is responsible for developing and publishing guidance on personal data breaches and must establish a mechanism for the reporting of such breaches.

23. Personal data breach notification to data subjects

(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the controller must in addition to notifying the Data Protection Supervisory Authority according to Section 22 also communicate the personal data breach to the data subject without undue delay.

(2) The communication to the data subject must describe in clear and plain language the nature of the personal data breach and recommend measures to address the personal data breach, including, where appropriate, the measures to mitigate the possible adverse effects of the breach.

(3) The communication of a personal data breach to the data subject is not required where:

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

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

(c) it would involve a disproportionate effort and the controller has made a public communication or similar measure whereby data subject is informed in an equally effective manner.

PART VI

TRANSBORDER FLOWS OF PERSONAL DATA

24. Transfer of Personal Data outside of Namibia

(1) Cross-border transfers of personal data to other countries and international organizations may not take place, unless an appropriate level of data protection is guaranteed. Such an appropriate level of protection may be secured by:

(a) the law of the receiving country or international organisation, including the adherence of that country or international organization to applicable international treaties or agreements; or

(b) ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing of personal data.

(2) The appropriateness of the level of protection afforded by the receiving country or international organization in question must be assessed in light of all the circumstances surrounding a data transfer. Particular consideration must be given to:

(a) the nature of the personal data to be transferred;

(b) the purpose and duration of the envisaged transfer;

(c) the data protection laws, both general and sectorial, in force in the receiving country or international organization in question;

(d) the recipient or recipients to whom the personal data are transferred.

(3) By way of derogation from subsection (1), cross-border transfers of personal data to other countries or international organisations which do not ensure an appropriate level of protection may take place only if:

(a) the data subject has given explicit, specific and free consent, after being informed of all risks arising with the transfer in the absence of appropriate safeguards;

(b) the specific interests of the data subject require the transfer in a particular case;

(c) the transfer is carried out in response to prevailing a legitimate interest, in particular an important public interest, which is provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society.

(d) the transfer constitutes a necessary and proportionate measure in a democratic society for the freedom of expression.; or

(e) the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

(4) The Data Protection Supervisory Authority shall be involved in assessing if any of the criteria are met when using the above-mentioned exceptions.

(5) The controller or processor shall document the assessment of the appropriate safeguards or the criteria referred to under subsection (3). The Data Protection Supervisory Authority shall be provided with all relevant information concerning the transfers referred to in subsections (3) and (4) and shall be entitled to request that the controller who transfers the data demonstrates the effectiveness of the safeguards or the existence of any of the criteria referred to in subsection (3).

(6) The Data Protection Supervisory Authority may, to protect the rights and fundamental freedoms of data subjects, prohibit transfers to other countries and international organisations, suspend them or subject them to additional conditions, other than the ones mentioned under this provision.

PART VII

DATA PROTECTION SUPERVISORY AUTHORITY

25. Establishment of the Data Protection Supervisory Authority of Namibia

There is hereby established an independent authority, to be known as the Data Protection Supervisory Authority of Namibia which is an independent administrative body. The Data Protection Supervisory Authority shall be appropriately empowered and equipped to safeguard the fundamental right to the protection of personal data and privacy of individuals, to oversee, monitor and enforce compliance with the provisions of this Act and to issue penalties and fines against any unlawful processing of personal data. The Data Protection Supervisory Authority shall treat the right to the protection of personal data and privacy of an individual as a fundamental human right.

26. Independence of the Data Protection Supervisory Authority

(1) The Data Protection Supervisory Authority shall act with independence and impartiality in performing its duties and exercising its powers. In doing so, the Data Protection Supervisory Authority shall neither seek nor accept external instructions.

(2) The Data Protection Supervisory Authority shall be provided with the resources necessary for the effective performance of its functions and the exercise of its powers under this Act.

(3) The Data Protection Supervisory Authority shall employ and have its staff which shall be subject to the exclusive direction of its Board.

(4) To ensure its financial independence, the Data Protection Supervisory Authority shall be equipped with sufficient technical and financial resources as well as the premises and infrastructure necessary for the effective performance of its tasks and the exercise of its powers, including those to be carried out in the context of international cooperation.

(5) The Data Protection Supervisory Authority shall prepare, present to Parliament and publish an annual report outlining its activities in a transparent and easily accessible manner.

(6) Decisions of the Data Protection Supervisory Authority may be subject to appeal through the courts.

27. Rules on the Establishment of the Data Protection Supervisory Authority

(1) The Data Protection Supervisory Authority shall be provided with the necessary resources to enable it to appoint skilled staff in the field of ICT technologies, security, law and digital technologies, to build internal capacity to enable the effective performance of its functions.

(2) The Data Protection Supervisory Authority shall consist of a Board of Directors and the general staff, which shall be distributed in units focusing on specific sectors of supervision. The Board shall consist of five members. The number of the general staff shall be set up in accordance with the workload of the authority.

(3) Each member or members of the Board and of the general staff of the Data Protection Supervisory Authority shall be subject to a duty of confidentiality and professional secrecy both during and after their term of office concerning any confidential information which has come to their knowledge in the course of the performance of their tasks or exercise of their powers.

(4) It shall be an offence of former or current members of staff who disclose personal data obtained during their duties, except under lawful authority.

28. Requirements for the Members of the Board of the Data Protection Supervisory Authority

(1) Each Member of the Board shall be appointed by a transparent meritocratic recruitment procedure. The Minister responsible for information and communication technology shall propose ten potential candidates to Parliament out of which Parliament shall select and appoint five as Members of the Board by simple majority voting.

(2) A Member of the Board shall have the qualifications, experience and skills, in particular in the area of the protection of personal data, required to perform his or her duties and exercise his or her powers.

(3) In particular, a Member of the Board must know and understand data protection law acquired from relevant professional experience and be qualified for judicial office or higher administrative service.

(4) The Members of the Board shall be non-executive members . In particular, they shall not be attached to Parliament, Government or any Ministry or other statutory body. Any Member of Parliament, Government or Ministry may only be appointed Member of the Data Protection Supervisory Authority 2 years after the termination of his or her office.

(5) To qualify for appointment, a proposed Member for the Board of the Data Protection Supervisory Authority shall, in particular:

(a) be a citizen of Namibia or permanently residing in Namibia;

(b) have no financial interest or be connected in any way that could impede his or her independence concerning his or her duties as a member of the Data Protection Supervisory Authority;

(c) shall be in full possession of his or her civil and political rights.

(6) A proposed Member of the Board of the Data Protection Supervisory Authority shall be disqualified for appointment, if:

(a) he or she has been adjudged or otherwise declared insolvent or bankrupt and has not been rehabilitated or discharged;

(b) he or she has, within a period of five years preceding the date of his or her proposed appointment, been convicted in Namibia or outside of Namibia of any crime that would be equivalent to a term of imprisonment imposed in Namibia without the option of a fine.

29. Terms of office and conditions of service of Members of the Board

(1) A Member of the Board shall hold office for a period not exceeding five years. The term of office of each member shall be renewable once.

(2) A Member of the Board shall continue in office after the expiry of his or her term until he or she has been re-appointed or his or her successor has been appointed.

(3) The duties of a Member of the Board shall end in the event of the expiry of the term of office, resignation, dismissal or compulsory retirement, as stipulated under Namibian law.

(4) A Member of the Board shall be dismissed by the Namibian Parliament only in cases of serious misconduct or if that Member no longer fulfils the conditions required for the performance of his or her duties as a member. Any dismissal shall be confirmed by simple majority voting in Parliament.

(5) In accordance with Namibian law, the office of a Member of the Board who vacates his or her office shall become vacant three months after the date upon which he or she gives notice in writing.

30. Requirements for the recruitment of the general staff of the Data Protection Supervisory Authority

(1) Each member of the general staff shall be recruited by a transparent meritocratic recruitment procedure by the Members of the Board and following the requirements to fulfil the duties of the Data Protection Supervisory Authority.

(2) Each member of the general staff shall have the qualifications, experience and skills, in particular, in the area of the protection of personal data, required to perform his or her duties and exercise his or her powers. In particular, members shall have an interest and shall be qualified in human rights law, cybersecurity, public administration, and information communication technology.

(3) The general staff shall be chosen for their experience and professional qualification in each of the following fields or areas of competence:

(a) information communication technology;

(b) data protection law;

(c) public administration.

31. Remuneration of the staff members of the Data Protection Supervisory Authority

The staff members of the Data Protection Supervisory Authority should be remunerated as deemed by their functions and to guarantee financial independence.

32. Competence of the Data Protection Supervisory Authority

(1) The Data Protection Supervisory Authority shall be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it by this Act.

(2) The Data Protection Supervisory Authority shall be competent for the supervision of both the processing of personal data carried out by public authorities and the processing of personal data carried out by private bodies.

(3) The Data Protection Supervisory Authority shall not be competent to supervise the processing of personal data of courts acting in their judicial capacity.

(4) The Data Protection Supervisory Authority shall be competent to take part in international cooperation with other Data Protection Supervisory Authorities.

33. Functions of the Data Protection Supervisory Authority

(1) Subject to this Act, the functions of the Supervisory Authority shall be:

(a) to promote and enforce fair processing of personal data as set out under this Act;

(b) to promote public awareness and understanding of the risks, rules, and rights concerning the processing of personal data. The Data Protection Supervisory Authority shall inform and provide information to data subjects regarding the exercise of their rights under this Act. Processing operations addressed to children and other vulnerable groups of people shall receive specific attention;

(c) to promote the awareness of controllers and processors of their obligations under this Act and advise upon request. In particular, the Data Protection Supervisory Authority shall advise on high-risk processing operations as defined and made publicly available by the Data Protection Supervisory Authority;

(d) to issue opinions either of its accords, or at the request of any person with a legitimate interest, on any matter relating to the application of the fundamental principles of the protection of privacy and personal data in the context of this Act;

(e) to monitor the application of this Act and any relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;

(f) to submit to the Court any administrative act which is not compliant with the fundamental principles of the protection of the privacy and the personal data protection;

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

(h) to conduct inquiries and investigations either of its own accord or at the request of a data subject or any other interested person or authority. The Data Protection Supervisory Authority may, concerning inquiries and investigations, call upon the assistance of experts;

(i) to receive, by post or electronic means or any another equivalent means, complaints lodged against a controller or processor;

(j) to investigate any complaint received in terms of this Act and to inform the complainant of the progress and the outcome of the investigation within a reasonable period;

(k) to explain to a data subject how he or she may pursue a complaint if the Data Protection Supervisory Authority fails to take appropriate steps to respond to a request or if the Data Protection Authority fails to act on a complaint within 3 months of the date on which it received the request;

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

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

(n) to perform the functions relating to trans-border transfers of personal data provided for under subsections 24(4), (5) and (6) , notably the approval of standardised safeguards referred to under subsection 24(1)(b);

(o) to encourage the drawing up of codes of conduct and internal rules concerning the processing of personal data and provide opinions and approve such codes of conducts and internal rules;

(p) to keep internal records of infringements of this Act; and

(q) to cooperate and share information with other supervisory authorities and participate in any international negotiations on matters of data protection.

(2) The performance of the tasks of the Data Protection Supervisory Authority shall be free of charge for data subjects.

(a) Where requests are manifestly unfounded or excessive, in particular because of their repetitive character, the supervisory authority may charge a reasonable fee based on administrative costs or refuse to act upon the request.

(b) The Data Protection Supervisory Authority may refuse a request if such request is not compatible with its powers or does not comply with the provisions of this Act.

(c) The supervisory authority shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

34. Powers of the Data Protection Supervisory Authority

(1) The Data Protection Supervisory Authority shall have:

(a) powers of investigation, intervention and enforcement;

(b) powers to issue opinions and approve statutory codes of conduct or guidelines relating to the processing of personal data;

(c) powers to issue decisions concerning violations of the provisions of this Act;

(d) powers to assist individuals to exercise their rights under this Act;

(e) powers to impose administrative sanctions and monetary fines;

(f) the power to institute legal proceedings or to bring any violations of the provisions of this Act to the attention of the competent judicial authorities of Namibia;

1. The Data Protection Supervisory Authority shall be consulted on proposals for any legislative or administrative measures which provide for the processing of personal data.

35. Penalties and fines imposed by the Data Protection Supervisory Authority

(1) The Data Protection Supervisory Authority may impose the following:

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

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

(c) a limitation on the processing until the lawfulness of processing may be established;

(d) a financial penalty to be calculated […].

(2) In case of a serious and immediate violation of the individual rights of a data subject, the Authority may:

(a) impose a ban on the processing of personal data, in particular on transfers of personal data;

(b) temporary or definitively restrict the processing of and access to personal data;

(3) The penalties and fines imposed by the Data Protection Supervisory Authority may be subject to appeal through the judicial authorities of Namibia.

36. Cooperation between Data Protection Supervisory Authorities

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

37. Funds of the Data Protection Supervisory Authority

(1) The Data Protection Supervisory Authority shall be funded partly by monies appropriated by Parliament and partly by way of charging fees payable by a controller, unless exempt as set out in this Act. The data protection registration fee shall be based on the financial turnover of a controller and the number of staff employed by that controller. Also, the Data Protection Supervisory Authority may collect the financial sanctions imposed against controllers.

(2) The Data Protection Supervisory Authority shall be allocated a separate and independent annual budget that shall consist of adequate financial resources to carry out its mandate.

(3) The budget of the Data Protection Supervisory Authority shall neither be subject to influence by Government during the initial allocation of funds nor concerning how the funds are spent.

(4) The annual budget of the Data Protection Supervisory Authority shall be authorized by Parliament. The Data Protection Supervisory Authority shall file its draft budget to Parliament within a timeframe that allows for an adequate assessment and decision of the proposed budget.

(5) The Data Protection Supervisory Authority shall be subject to the financial control of the Auditor General.

(6) The budget of the Data Protection Supervisory Authority shall be shown in a separate heading in the general budget of Namibia.

PART VIII
OFFENCES AND PENALTIES

38. . Specific Offences

(1.) Unlawful obtaining of personal data

(2.) It is an offence for a person to knowingly or recklessly obtain, retain, disclose or procure the disclosure of personal data without the authorisation of the controller.

(3.) It is a defence for a person charged with an offence under paragraph (1) to prove that the obtaining, disclosure, procuring or retaining of the personal data was:

(a) necessary for the investigation and prosecution of a specific criminal offence;

(b) was required or authorised by law or by the order of a court;

(c) was justified as being in the public interest.

(4.) It is also a defence for a person charged with an offence under paragraph (1) to prove that:

(a) they acted in the reasonable belief that they had a legal right to obtain, disclose, procure or retain the personal data; or

(b) the person acted in the reasonable belief that the controller would have authorised the obtaining, disclosure, procuring or retaining of the personal data.

39. Alteration of personal data to prevent disclosure to a data subject

Where a data subject exercises his or her right of access under this Act, and makes a request of a controller for access to, or a copy of their personal data, it is an offence for a controller or where applicable a processor, or a person employed by a controller, to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information to a person making a request and that the person is entitled to receive under a right of access to personal data.