No. of 2019

VIRGIN ISLANDS

DATA PROTECTION ACT, 2019

ARRANGEMENT OF SECTIONS

Section

No. of 2019 **Data Protection Act, 2019** **Virgin Islands**

I Assent

Governor
, 2019

VIRGIN ISLANDS

No. of 2019

A Bill for

AN ACT to provide for the protection of personal data processed by public and private bodies and for related matters.

[Gazetted , 2019]

ENACTED by the Legislature of the Virgin Islands as follows:

PART I
PRELIMINARY

Short title and commencement.

1. (1) This Act may be cited as the Data Protection Act, 2019.

(2) This Act shall come into force on such date as the Minister may, by Notice published in the *Gazette,* appoint, and different dates may be appointed for different provisions of this Act.

Interpretation.

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

"alternative format" means, with respect to personal data, a format that allows a person with a sensory disability to read or listen to the personal data;

"authorised officer" means a person to whom the functions of the Information Commissioner have been delegated pursuant to section 41;

"Chief Executive Officer" means the officer for the time being exercising the highest level of administrative functions within a public body or private body;

"commercial transactions" means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance;

"Court" means the High Court;

"data processor", in relation to personal data, means a person who, processes data on behalf of a data user, but does not include an employee of the data user;

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

"data user" means a person who either alone or jointly or in common with other persons processes any personal data, or has control over, or authorises the processing of any personal data, but does not include a data processor;

"document" includes

(a) any medium in which data is recorded, whether printed, or on tape, or film or by electronic means, or otherwise;

(b) map, diagram, photograph, film, microfilm, video-tape, sound recording, or machine readable record;

(c) any record which is capable of being produced from

(i) a machine-readable record by means of equipment or a programme, or a combination of both, or

(ii) any equipment or a programme, or a combination of both,

and is used for that purpose by the public body or private body which holds the record;

"Information Commissioner" means the person appointed as such pursuant to section 24;

"Minister" means the Minister to whom responsibility for information is assigned;

"personal data" means any information in respect of commercial transactions, which

(a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or

(c) is recorded as part of a relevant filing system or with the intention

that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information, or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject;

"private body" means a body, excluding a public body, that

(a) carries on any trade, business or profession, but only in that capacity; or

(b) has legal personality;

"processing", in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including the

(a) organisation, adaptation or alteration of personal data;

(b) retrieval, consultation or use of personal data;

(c) disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or

(d) alignment, combination, correction, erasure or destruction of personal data;

"public body" includes

(a) the House of Assembly or any committee of the House of Assembly;

(b) the Cabinet of the Virgin Islands;

(c) a Ministry, department, or division of the Ministry;

(d) a local authority;

(e) a statutory body established for a public purpose, whether incorporated or not, and which is owned or controlled by the Government;

(g) any other body prescribed by the Minister, to be a public body for the purposes of this Act; and

"sensitive personal data" means any personal data about a data subject's

(a) physical condition or mental health condition;

(b) sexual orientation;

(c) political opinions;

(d) religious beliefs or other beliefs of a similar nature;

(e) commission or alleged commission, of any offence; or

(f) any other personal data that the Minister may by Order prescribe;

Objects of Act.

3. The objects of this Act are to

(a) safeguard personal data processed by public bodies and private bodies by balancing the necessity of processing the personal data protecting personal data from unlawful processing by public bodies and private bodies; and

(b) to promote transparency and accountability in the processing of personal data.

Application of Act.

4. (1) With respect to a private body, this Act applies to a

(a) person who processes; or

(b) person who has control over, or authorises, the processing of

any personal data in respect of commercial transactions.

(2) Subject to subsection (1), this Act applies to a person in respect of personal data if

(a) the person is established in the Virgin Islands and processes personal data, or employs or engages any other person to process personal data on his or her behalf, whether or not in the context of that establishment; or

(b) the person is not established in the Virgin Islands, but uses equipment in the Virgin Islands for processing personal data otherwise than for the purposes of transit through Virgin Islands.

(3) A person referred to in subsection (2)(b) shall nominate for the purposes of this Act a representative established in the Virgin Islands.

(4) For the purposes of subsections (2) and (3), each of the following shall be treated as established in the Virgin Islands:

(a) a person who is physically in the Virgin Islands for a period of not less than one hundred and eighty days in one calendar year;

(b) a body incorporated under any written laws in the Virgin Islands;

(c) a partnership or other unincorporated association formed under any written laws in the Virgin Islands; and

(d) a person who does not fall within paragraph (a), (b) or (c) but maintains in Virgin Islands

(i) an office, branch or agency through which he or she carries on any activity; or

(ii) a regular professional practice.

Saving of certain laws.

5. This Act shall not affect the operation of a law that makes provision with respect to the processing of personal data and is capable of operating concurrently with this Act.

Act to bind the Crown.

6. This Act binds the Crown.

PART II
PRIVACY AND DATA PROTECTION PRINCIPLES

General Principle.

7. (1) A data user shall not

(a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his or her consent to the processing of the personal data; or

(b) in the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with section 20.

(2) Notwithstanding subsection (1)(a) and subject to subsection (3), a data user may process personal data about a data subject if the processing is necessary

(a) for the performance of a contract to which the data subject is a party;

(b) for the taking of steps at the request of the data subject with a view to entering into a contract;

(c) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;

(d) in order to protect the vital interests of the data subject;

(e) for the administration of justice; or

(f) for the exercise of any functions conferred on a person by or under any law.

(3) Personal data shall not be processed unless

(a) the personal data is processed for a lawful purpose directly related to an activity of the data user;

(b) the processing of the personal data is necessary for, or directly related to that purpose; and

(c) the personal data is adequate but not excessive in relation to that purpose.

Notice and Choice Principle.

8. A data user shall inform a data subject upon a request for personal data

(a) of the purposes for which the personal data is being or is to be collected and further processed;

(b) of any information available to the data user as to the source of that personal data;

(c) of the data subject's right to request access to and to

request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data;

(d) of the class of third parties to whom the data user discloses or may disclose the personal data;

(e) whether it is obligatory or voluntary for the data subject to supply the personal data; and

(f) where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he or she fails to supply the personal data.

Disclosure Principle.

9. Subject to section 19, no personal data shall, without the consent of the data subject, be disclosed

(a) for any purpose other than

(i) the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or

(ii) a purpose directly related to the purpose referred to in subparagraph (i);

(b) to any party other than a third party of the class of third parties as specified in section 8(d).

Security Principle.

10. (1) A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard to

(a) the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction;

(b) the place or location where the personal data is stored;

(c) any security measures incorporated into any equipment in which the personal data is stored;

(d) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and

(e) the measures taken for ensuring the secure transfer of the personal data.

(2) Where processing of personal data is carried out by a data processor on behalf of the data user, the data user shall, for the purpose of protecting the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction, ensure that the data processor

(a) provides sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and

(b) takes reasonable steps to ensure compliance with those measures.

Retention Principle.

11. (1) The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.

(2) The data user shall take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.

Data Integrity Principle.

12. A data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.

Access Principle.

13. A data subject shall be given access to his or her personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this Act.

PART III
RIGHTS OF DATA SUBJECTS

Right of access to personal data.

14. (1) Subject to subsection (2), a public body or a private body shall, on the written request of a data subject for access to personal data, inform the data subject

(a) whether his or her personal data is being processed by or on behalf of that body;

(b) if personal data is being processed by or on behalf of that body, communicate to the data subject in an intelligible form a description of

(i) the personal data relating to that person which is being or will be processed;

(ii) the purposes for which the personal data is being or will be processed;

(iii) the recipients or classes of recipients to whom personal data is or may be disclosed; and

(iv) any information available to that body as to the source of the data.

(c) within thirty days after the request is received, whether or not access will be given to all or part of the personal data.

(2) Where the public body or the private body decides to grant access to the personal data requested pursuant to subsection (1), the Chief Executive Officer shall inform the data subject, in writing, of its decision and on payment of the prescribed fee provide access to the information.

Extension of time where access is requested.

15. (1) A Chief Executive Officer may extend the time limit for compliance with a request for access to personal data

(a) by not more than thirty days if

(i) meeting the original time limit would unreasonably interfere with the operations of the public body or private body; or

(ii) consultations are necessary to comply with the request that cannot be reasonably be completed within the original time limit; or

(b) by such period of time as is reasonable, if the additional time is necessary for converting the personal data into an alternative format.

(2) Where a Chief Executive Officer extends the time limit for compliance pursuant to subsection (1), he or she shall, give notice in writing of the extension to the person who made the request stating in the notice

(a) the length of the extension; and

(b) informing the person that he or she has a right to make a complaint to the Information Commissioner about the extension.

Denial of access to personal data.

16. (1) A public body or a private body is not obliged to comply with a request for access to personal data

(a) unless it is supplied with such information as it may reasonably require in order to satisfy itself as to the identity of the person making the request and to locate the personal data which that person seeks;

(b) if compliance with the request will be in contravention of the exemptions contained in Part IV or of any duty of confidentiality recognised by law;

(c) where another person who can be identified from the personal data consents to the disclosure of his or her personal data to the person making the request; or

(d) where the body obtains the written approval of the Information Commissioner.

(2) Where a public body or a private body refuses to give access to personal data, its Chief Executive Officer shall notify the data subject, in writing, stating in the notice given

(a) that the personal data does not exist; or

(b) the specific provision of this Act on which refusal was based or the provision on which a refusal could reasonably be expected to be based if the personal data existed, and that the person who made the request has the right to make a complaint to the Information Commissioner about the refusal.

(3) Where a Chief Executive Officer fails to give access to personal data requested under section 14 within the time limits set out in section 14(1)(c) or as extended in section 15 he or she shall, for the purposes of this Act, be deemed to have refused to give access.

Form of access.

17. (1) Where a data subject is to be given access to personal data requested pursuant to section 14, the public body or private body shall

(a) permit the data subject to examine the personal data; or

(b) provide the data subject with a copy of the personal data.

(2) Where access to personal data is given under this Act and the data subject to whom access is to be given has a sensory disability and requests that access be given in an alternative format, access shall be given in an alternative format if

(a) the personal data already exists under the control of a public body or a private body in an alternative format that is acceptable to the person; or

(b) the Chief Executive Officer considers it to be reasonable to cause the personal data to be converted to an alternative format.

Rectification of personal data.

18. (1) Where a data subject informs a public body or a private body that the personal data processed by that body is

(a) incomplete, incorrect, misleading, or excessive; or

(b) not relevant to the purpose for which the document is held,

the body shall, require the data subject to submit an application requesting that the data be amended.

(2) An application under subsection (1) shall

(a) be in writing; and

(b) as far as practicable, specify

(i) the document containing the record of personal data that is claimed to require the amendment;

(ii) the personal data that is claimed to be incomplete, incorrect, misleading or irrelevant;

(iii) the reasons for the claim; and

(iv) the amendment requested by the data subject.

(3) Where a public body or a private body is satisfied with the reasons for an application made pursuant to subsection (1), that body shall cause the personal data to be amended and to the extent that it is practicable to do so, when

making an amendment to personal data pursuant to this section, ensure that it does not obliterate the text of the document as it existed prior to the amendment.

(4) Where a public body or a private body is not satisfied with the reasons for an application pursuant to subsection (1), it may refuse to make an amendment to the personal data and shall notify the data subject in writing, of the reasons for the refusal and inform the data subject of the right to lodge a complaint with the Information Commissioner.

(5) A data subject who is aggrieved by a decision of a public body or a private body pursuant to subsection (4) may lodge a complaint in writing to the Information Commissioner within twenty-eight days of receipt of the refusal.

Extent of disclosure of personal data.

19. Notwithstanding section 9, personal data of a data subject may be disclosed by a data user for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances:

(a) the data subject has given his or her expressed consent to the disclosure;

(b) the disclosure

(i) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations; or

(ii) was required or authorised by or under any law or by the order of a court;

(c) the data user acted in the reasonable belief that he or she had in law the right to disclose the personal data to the other person;

(d) the data user acted in the reasonable belief that he or she would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or

(e) the disclosure was justified as being in the public interest in circumstances as determined by the Minister.

Processing of sensitive personal data.

20. (1) Subject to subsection (2) and Part II, a data user shall not process any sensitive personal data of a data subject unless

(a) the data subject has given his or her explicit consent to the processing of the personal data;

(b) the processing is necessary

(i) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data user in connection with employment;

(ii) in order to protect the vital interests of the data subject or another person, in a case where

(A) consent cannot be given by or on behalf of the data subject;

(B) the data user cannot reasonably be expected to obtain the consent of the data subject; or

(C) consent by or on behalf of the data subject has been unreasonably withheld;

(iii) for medical purposes and is undertaken by

(A) a healthcare professional; or

(B) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;

(iv) for the purpose of, or in connection with, any legal proceedings;

(v) for the purpose of obtaining legal advice;

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

(vii) for the administration of justice;

(viii) for the exercise of any functions conferred on any person by or under any enactment; or

(ix) or any other purposes as the Minister thinks fit; or

(c) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

(2) The Minister may by Order published in the *Gazette* exclude the application of subsection (1)(b)(i), (vii) or (viii) in such cases as may be specified in the Order, or provide that, in such cases as may be specified in the Order, the condition in subsection (1)(b)(i), (vii) or (viii) is not to be regarded as satisfied unless such further conditions as may be specified in the Order are also satisfied.

(3) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding two years or, both.

(4) For the purposes of this section

"medical purposes" includes preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of healthcare services;

"healthcare professional" includes a registered medical practitioner, registered dental practitioner, pharmacist, any registered allied health practitioner, registered nurse and any other person involved in providing healthcare services under any law relating to health.

PART IV
EXEMPTION

Exemption.

21. (1) This Act shall not apply to personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes.

(2) Subject to section 22, personal data

(a) processed for

(i) the prevention or detection of crime or for the purpose of investigations;

(ii) the apprehension or prosecution of offenders; or

(iii) the assessment or collection of any tax or duty or any other imposition of a similar nature,

shall be exempted from the General Principle, Notice and

Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act;

(b) processed in relation to information of the physical or mental health of a data subject shall be exempted from the Access Principle and other related provisions of this Act of which the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other individual;

(c) processed for preparing statistics or carrying out research shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;

(d) that is necessary for the purpose of, or in connection with any order or judgment of a court shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act;

(e) processed for the purpose of discharging regulatory functions shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle and Access Principle and other related provisions of this Act if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; or

(f) processed only for journalistic, literary or artistic purposes shall be exempted from the General Principle, Notice and Choice Principle, Disclosure Principle, Retention Principle, Data Integrity Principle and Access Principle and other related provisions of this Act, provided that

(i) the processing is undertaken with a view to the publication by a person of the journalistic, literary or artistic material;

(ii) the data user reasonably believes that, taking into account the special importance of public interest in freedom of expression, the

publication would be in the public interest; and

(iii) the data user reasonably believes that in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the journalistic, literary or artistic purposes.

Power to make further exemptions.

22. The Minister may, upon the recommendation of the Information Commissioner, and by Order published in the *Gazette* exempt

(a) the application of any of the Personal Data Protection Principles under this Act to any data user or class of data users; or

(b) any data user or class of data users from all or any of the provisions of this Act.

PART V
INFORMATION COMMISSIONER

Office of the Information Commissioner.

23. There is established by this Act an office to be known as the Office of the Information Commissioner.

Appointment of Information Commissioner and other staff.

24. (1) The Governor, acting in accordance with section 92 of the Constitution, shall appoint a suitably qualified person to be the Information Commissioner and such other staff as may be necessary for the efficient administration of this Act.

(2) A person appointed under subsection (1) shall

(a) have training at least 10 years' experience in law, economics, finance, information security, technology, audit or human resource management; and

(b) hold office for five years and is eligible for reappointment.

Functions of Information Commissioner.

25. The functions of the Information Commissioner include

(a) monitoring compliance by public and private bodies with the requirements of this Act;

(b) providing advice to public bodies and private bodies on their obligations under this Act;

(c) receiving and investigating complaints about alleged violations of the data protection principles and in respect thereof, may make reports to complainants;

(d) undertaking educational programmes to promote understanding of this Act;

(e) undertaking research into, and monitoring developments in data processing and information technology to ensure the continued protection of personal data through administrative, legislative or other methods, and to report to the Minister the results of such research and monitoring; and

(f) exercising and performing such other functions as are conferred or imposed on the Information Commissioner by or under this Act or any other enactment.

Powers of Information Commissioner.

26. The Information Commissioner shall have powers, for the purpose of carrying out his or her functions, to do all such acts as are necessary for or in connection with the carrying out of these functions.

PART VI
ENFORCEMENT

Investigation of complaints.

27. (1) The Information Commissioner may, on a complaint made by a data subject or at the instance of the Information Commissioner, investigate or cause to be investigated whether any provisions of this Act have been, are being or are likely to be contravened by a public body or a private body in relation to a data subject.

(2) Where a complaint is made to the Information Commissioner under subsection (1), the Information Commissioner shall

(a) investigate or cause the complaint to be investigated by an authorised officer, unless the Information Commissioner is of the opinion that it is frivolous or vexatious; and

(b) as soon as is reasonably practicable, notify the data subject in writing of his or her decision in relation to the complaint and that the data subject may, if aggrieved by the Information Commissioner's decision, appeal to the Court against the decision.

(3) Nothing in this Act precludes the Information Commissioner from receiving and investigating complaints of a nature described in subsection (1) that are submitted by a person authorised by the data subject to act on behalf of the

data subject, and a reference to a complainant in any other section includes a reference to a person so authorised.

Form of complaint.

28. (1) A complaint pursuant to this Act shall be made to the Information Commissioner in writing unless the Information Commissioner authorises otherwise.

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

Notice of investigation.

29. Before commencing an investigation of a complaint pursuant to this Act, the Information Commissioner shall notify the Chief Executive Officer of the intention to carry out the investigation and shall include in the notification the substance of the complaint.

Information notice.

30. The Information Commissioner may, by an information notice served on a person, request that person to furnish to him or her, in writing, within a time specified

(a) access to personal data;

(b) information about and documentation of the processing of personal data;

(c) information related to the security of processing of personal data; and

(d) any other information in relation to matters specified in the notice as is necessary or expedient for the performance by the Information Commissioner of his or her functions and exercise of his or her powers and duties under this Act.

Warrant to enter and search.

31. (1) If a Magistrate is satisfied by information on oath supplied by the Information Commissioner or an authorised officer that there are reasonable grounds for suspecting that 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 by the Information Commissioner or an authorised officer, the Magistrate may issue a warrant authorising the entry and search of said premises.

(2) The Information Commissioner or an authorised officer who is accompanied by a police officer may, upon the authority of a warrant issued by a Magistrate, at any time enter any premises, for the purpose of discharging any functions or duties under this Act.

Enforcement notice.

32. (1) Where the Information Commissioner is satisfied that a public body or a private body has contravened or is contravening this Act, the Information Commissioner shall, subject to subsection (2) serve an enforcement notice on the relevant body, requiring it to take such steps as are specified in the enforcement notice within such time as may be specified in the notice.

(2) An enforcement notice shall

(a) specify the provision of this Act that, has been contravened or is being contravened and the reasons for the Information Commissioner serving the notice; and

(b) specify the action which the Information Commissioner requires the public body or private body to take to correct the contravention.

(3) An enforcement notice may require the public body or private body

(a) to rectify or erase personal data; or

(b) to supplement the personal data with statements concerning the matters dealt with by the personal data as the Information Commissioner may approve.

(4) A public body or a private body it shall, as soon as practicable, and in any event not later than thirty days after complying with enforcement notice, notify

(a) the data subject concerned; and

(b) any person, where the Information Commissioner considers it reasonably practicable to do so, to whom the personal data was disclosed twelve months before the date of the service of the enforcement notice and ending immediately before such compliance,

of the rectification or erasure made, if the compliance materially modifies the personal data concerned.

(5) The Information Commissioner may cancel or vary an enforcement notice and, if he or she does so, shall in writing notify the public body or private body on whom it was served of the cancellation.

Assessment of processing.

33. (1) The Information Commissioner may from time to time at his or her discretion, or upon a request made by or on behalf of a person who is, or believes

himself or herself to be, directly affected by the processing of personal data by a public body or a private body, carry out an assessment of the processing of personal data to determine whether it is carried out in compliance with this Act.

(2) The Information Commissioner shall conduct an assessment in such manner as appears to him or her to be appropriate.

(3) If following an assessment under subsection (1), the Information Commissioner considers that a public body or a private body has not complied with the provisions of this Act, the Information Commissioner shall provide the Chief Executive Officer of the public body or private body with a report containing the findings of the assessment and any recommendations that the Information Commissioner considers appropriate.

(4) A report made by the Information Commissioner under subsection (3) may be included in a report made to House of Assembly pursuant to this Act.

Civil remedies.

34. (1) A data subject who suffers damage by reason of the contravention by a public body or private body of any of the provisions of this Act may institute civil proceedings in the Court.

(2) In proceedings brought against a public body or a private body by virtue of this section, it is a defence to prove that it has taken such care as in all the circumstances was reasonably required, to comply with the requirement concerned.

Whistle-blower's protection.

35. An employer whether or not a public body, shall not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee or deny that employee a benefit, because

(a) the employee acting in good faith, and on the basis of reasonable belief has

(i) notified the Commissioner that the employer or any other person has contravened or is about to contravene this Act;

(ii) done or stated the intention of doing anything that is required to be done in order to avoid having any person contravene this Act; or

(iii) refused to do or stated the intention of refusing to do anything that is in contravention of this Act; or

(b) the employer believes that the employee will do anything referred to in paragraph (a).

PART VII
OFFENCES

Obstruction.

36. A person who wilfully obstructs the Information Commissioner or an authorised officer in the conduct of his or her duties and functions under this Act commits an offence and is liable on summary conviction to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding six months, or both.

37. (1) A person who

Willful disclosure of information.

(a) willfully discloses personal information in contravention of this Act; or

(b) collects, stores or disposes of personal information in a manner that contravenes this Act,

commits an offence and is liable on summary conviction to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding six months or, both.

Breach of confidentiality.

38. A person who breaches the confidentiality obligations established under section 44, commits an offence and is liable on

(a) summary conviction, to a fine of not exceeding fifty thousand dollars or to imprisonment for a term not exceeding three years, or both; and

(b) conviction on indictment, to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding five years, or both.

Offence by bodies corporate.

39. (1) Where an offence under this Act is committed by a body corporate, and is proved to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, any director, manager, secretary or other similar officer of that body corporate, or a person purporting to act in that capacity, the person as well as the body corporate each commits the offence and are liable to be proceeded against and punished accordingly.

(2) A body corporate that commits an offence under this Act is liable on

(a) summary conviction, to a fine of not exceeding two hundred and fifty thousand dollars; and

(b) conviction on indictment, to a fine not exceeding five

hundred thousand dollars.

PART VIII
MISCELLANEOUS

Right of Appeal.

40. Any person who is aggrieved by a decision of the Information Commissioner may, within thirty days of receiving written notice of the decision, appeal to the High Court.

Delegation.

41. The Information Commissioner may delegate any power or function conferred upon him or her by this Act to an authorised officer subject to such restrictions as the Information Commissioner may specify.

Oath of office.
Schedule

42. A person appointed under section 24(1) shall, before he or she performs the functions of Information Commissioner, take and subscribe to the oath of office set out in the Schedule.

Immunity.

43. (1) No civil or criminal proceedings shall lie against the Information Commissioner or any person acting under the direction of the Information Commissioner, for anything done or omitted, in good faith, in the course of the discharge or purported discharge of any functions, duties or powers under this Act.

(2) For the purpose of any law relating to libel or slander

(a) anything said, any information supplied or any document or thing produced in good faith in the course of an investigation carried out by or on behalf of the Information commissioner under this Act is absolutely privileged; and

(b) any report made in good faith by the Information Commissioner under this Act is absolutely privileged.

Confidentiality.

44. Subject to this Act, the Information Commissioner and every person acting on behalf of or under the direction of the Information Commissioner shall not disclose any information that comes to their knowledge in the conduct of their functions under this Act.

Annual report.

45. (1) The Information Commissioner shall prepare and submit to the Minister, no later than three months after the end of the financial year, an annual report relating to the activities of the Office of the Information Commissioner during the preceding year and the Minister shall cause the report to be laid before the House of Assembly.

(2) Notwithstanding subsection (1), the Information Commissioner may, at any time, make a special report to the Minister referring to and

commenting on any matter within the scope of the powers and functions of the Information Commissioner where, in the opinion of the Information Commissioner, the matter is of such urgency or importance that a report should not be deferred until the time provided for transmission of the next annual report prepared pursuant to subsection (1).

(3) Where the Minister receives a report from the Information Commissioner pursuant to subsection (2), the Minister shall cause the report to be laid before the House of Assembly.

Power to amend Schedule.

46. The Minister may, amend the Schedule by Order published in the *Gazette*.

Regulations.

47. (1) The Minister may, with the approval of Cabinet, make regulations for giving effect to the provisions of this Act.

(2) Without prejudice to the generality of subsection (1), regulations made under this section may prescribe

(a) guidelines for the disposal of personal data held by a public body or a private body;

(b) special procedures for giving a person access pursuant to section 17, to personal data;

(c) codes of practice; and

(d) anything that is required to be prescribed by this Act.

(3) Any regulations made pursuant to subsection (1) shall be subject to negative resolution of the House of Assembly.

SCHEDULE

[Section 41]

OATH / AFFIRMATION FOR INFORMATION COMMISSIONER

I, do swear (or solemnly affirm) that I will faithfully execute my duties as Information Commissioner in the Office of the Information Commissioner in accordance with the requirements of **Data Protection Act, 2019** without fear or favour, affection or ill-will and that in the execution of the functions of that office I will not,

I further solemnly swear / affirm that, except as provided by law, I will not disclose to any unauthorised person or persons the nature or content of any document which may come to my knowledge in the course of my duties as Information Commissioner.

.

So help me God (To be omitted in affirmation).

Sworn/Declared before me this……day of……..20 .

Passed by the House of Assembly this day of , 2019.

Speaker.

Clerk of the House of Assembly.

OBJECTS AND REASONS

This Bill seeks to establish a legal framework that would ensure that the protection of personal data collected and processed by public and private bodies. Advances in technology make it easier to gather, disseminate and manipulate vast amount of personal data. This Bill is necessary, as the government seeks to strengthen e-government services and electronic commerce in the Territory.

The Bill consists of 8 parts.

PART I (Clauses 1 – 6) would deal with matters of a preliminary nature.

Clause 1 provides for the short title and commencement provision.

Clause 2 would define certain words and expressions used in order to ensure that the intended purpose of the legislation is achieved.

Clauses 3 and 4 would set out the objects and application of the Bill respectively.

Clause 5 would provide for the saving of certain laws, whilst clause 6 would provide for the Act to bind the crown.

PART II (Clauses 7 – 13) contains seven privacy and data protection principles: the general principle, the notice and choice principle, the disclosure principle, the security principle, the retention principle, the data integrity principle and the access principle.

PART III (Clauses 14 – 20) would provide for the rights of data subjects. These rights include access to personal data and rectification of personal data.

PART IV (Clauses 21 – 22) would deal with exemptions for personal data processed by a person only for the purpose of that individual's personal, family or household affairs. It would also provide for the Minister to make further exemptions by Order.

PART V (Clauses 23 – 26) would provide for the establishment of the Office of the Information Commissioner, the appointment of the Information Commissioner and the functions and powers of the Information Commissioner.

PART VI (Clauses 25- 35) would specify the enforcement powers of the Information Commissioner. These powers include the investigation of complaints and the issuance of notices. Persons who suffer damage caused by unlawful processing of data may apply to the Court for remedies.

Clause 35 would provide for the protection for persons who divulge information about breaches of this Act in their organisation. An employer would therefore be

prohibited from dismissing, suspending, demoting, disciplining, harassing or otherwise disadvantaging an employee or denying the employee of any benefit.

Part VII (Clauses 36-39) would set out the offences under this Act.

Clause 36 would make it an offence to wilfully obstruct the Information Commissioner or an authorised officer in the execution of his or her functions.

Clause 37 would make it an offence for a person to wilfully disclose information or maintain a personal information bank in contravention of this Act.

Clause 38 would make it an offence for a person to breach the confidentiality obligations under section 44.

Clause 39 would provide for offences by bodies corporate.

PART VIII (Clauses 40 - 47) would deal with miscellaneous matters.

Clause 40 would provide for a right of appeal from decisions of the Information Commissioner.

Clauses 41 and 42 would provide for the delegation of the powers of the Information Commissioner and the execution of the oath of office, respectively.

Clause 43 and 44 would provide for the protection from civil or criminal proceedings for actions done in good faith in the course of the discharge of any functions under the Act and confidentiality with respect to information that comes within the knowledge of the Information Commissioner.

Clause 47 would provide for and regulation making powers.

Premier.