I assent,

SAMUEL WEYMOUTH TAPLEY SEATON

Governor-General

23rd May, 2018.

SAINT CHRISTOPHER AND NEVIS

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

[*Published 7th June 2018, Official Gazette No. 31 of 2018.*]

BE IT ENACTED by the Queen's Most Excellent Majesty, by and with the advice and consent of the National Assembly of Saint Christopher and Nevis and by the authority of the same as follows:

PART I
PRELIMINARY

1. Short title and commencement.

(1) This Act may be cited as the Data Protection Act, 2018.

(2) This Act shall come into force on a day to be fixed by the Minister by Order published in the *Gazette*.

2. Interpretation.

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;

"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;

"correct" means, in relation to personal data, to alter the data by way of amendment, deletion, or addition;

"Court" means the Eastern Caribbean Supreme Court;

"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" means any medium in which data is recorded, whether printed or on tape or film or by electronic means or otherwise and also means any map, diagram, photograph, film, microfilm, video-tape, sound recording, or machine readable record or any record which is capable of being produced from a machine-readable record by means of equipment or a programme, or a combination of both, which is used for that purpose by the public body or private body which holds the record; equipment or a programme, or a combination of both, which is used for that purpose by the public body or private body which holds the record;

"Information Commissioner" means the Commissioner appointed pursuant to section 35 of the Freedom of Information Act;

"Minister" means the Minister with responsibility for justice;

"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–

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

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

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

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

"public body" includes–

(a) Parliament or any committee of Parliament;

(b) the Cabinet as constituted under the Constitution;

(c) a ministry, a department or a division of the ministry or a constituency office of a minister, wherever located;

(d) a local authority;

(e) a public statutory corporation or body;

(f) a body corporate or an incorporated public body established for a public purpose, which is owned or controlled by the State;

(g) an embassy, consulate or mission of the Saint Christopher and Nevis or an office of the Saint Christopher and Nevis situate outside Saint Christopher and Nevis whose functions include the provision of diplomatic or consular services for or on behalf of Saint Christopher and Nevis;

(h) any other body designated by the Minister by Regulations made under this Act, to be a public body for the purposes of this Act.

"sensitive personal data" means any personal data consisting of information as to the physical or mental health or condition of a data subject, his or her sexual orientation, his or her political opinions, his or her religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him or her of any offence or any other personal data as the Minister may determine by order published in the *Gazette*.

3. Objects of Act.

The objects of this Act are to safeguard personal data processed by public bodies and private bodies in an era in which technology increasingly facilitates the processing of personal data by balancing the necessity of –

(a) processing personal data by public bodies and private bodies; and

(b) safeguarding personal data from unlawful processing by public bodies and private bodies;

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

4. Application of Act.

(1) With respect to a private body this Act applies to a person who processes or 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 Saint Christopher and Nevis and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or

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

(3) A person falling within paragraph (2)(b) shall nominate for the purposes of this Act a representative established in Saint Christopher and Nevis.

(4) For the purposes of subsections (2) and (3), each of the following is to be treated as established in Saint Christopher and Nevis:

(a) an individual whose physical presence in Saint Christopher and Nevis shall not be less than one hundred and eighty days in one calendar year;

(b) a body incorporated under the Companies Act, Cap 21.03;

(c) a partnership or other unincorporated association formed under any written laws in Saint Christopher and Nevis; and

(d) a person who does not fall within paragraph (a), (b) or (c) but maintains in Saint Christopher and Nevis –

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

(ii) a regular professional practice.

5. Saving of certain laws.

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.

6. Act to bind the State.

This Act shall bind the State.

PART II
PRIVACY AND DATA PROTECTION PRINCIPLES

7. General Principle.

(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 the provisions of section 20.

(2) Notwithstanding paragraph (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.

8. Notice and Choice Principle.

A data user shall inform a data subject upon a request for personal data–

(a) 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.

9. Disclosure Principle.

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).

10. Security Principle.

(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–

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

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

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

(e) to 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.

11. Retention Principle.

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

(2) It shall be the duty of a data user to 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.

12. Data Integrity Principle.

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.

13. Access Principle.

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

14. Right of access to personal data.

Subject to the provisions of this Act, a public body or a private body shall, on the written request of and the payment of the prescribed fee by a person for access to personal data–

(a) inform the person whether personal data of which that person is the data subject 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 person in an intelligible form a description of–

(i) the personal data of which that person is the data subject;

(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 the body as to the source of the data.

15. Notice and time where access is requested.

(1) Subject to section 16, where access to personal data is requested under section 14, the public body or private body to which the request is made shall, subject to subsection (2), within thirty days after the request is received –

(a) give written notice to the person who made the request as to whether or not access to the personal data or a part thereof will be given; and

(b) if access is to be granted, give to the person who made the request access to the personal data or a part thereof.

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

(a) by a maximum of thirty days if–

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

(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;

by giving notice of the extension and the length of the extension to the person who made the request within thirty days after the request is received, and a statement that the person has a right to make a complaint to the Information Commissioner about the extension.

16. Denial of access to personal data.

(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 state in the notice given pursuant to section 15 (2)(a)–

(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 this Act, he or she shall, for the purposes of this Act, be deemed to have refused to give access.

17. Form of access.

(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.

18. Right of rectification of personal data.

(1) Where personal data that is processed by a public body or a private body to which access has been given, contains personal data which the data subject claims-

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

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

the body shall, upon application of the data subject, cause the data to be amended upon being satisfied of the claim.

(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) To the extent that it is practicable to do so, the public body or private body shall, when making an amendment to personal data in a document 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 inform the data subject of its refusal and the reasons for the refusal and inform the data subject that they may lodge a complaint in writing to 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 the date of the receipt of the communication of refusal.

19. Extent of disclosure of personal data.

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 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.

20. Processing of sensitive personal data.

(1) Subject to subsection (2) and Part II, a data user shall not process any sensitive

personal data of a data subject except in accordance with the following conditions–

(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; or

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

(iii) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;

(iv) 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;

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

(vi) for the purpose of obtaining legal advice;

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

(viii) for the administration of justice;

(ix) for the exercise of any functions conferred on any person by or under any written law; or

(x) 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 subparagraph (1)(b)(i), (viii) or (ix) 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 subparagraph (1)(b)(i), (viii) or (ix) 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 shall, on conviction, be liable to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding two years or to both.

(4) For the purposes of this section–

"medical purposes" includes the purposes of preventive medicine, medical

diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of healthcare services;

"healthcare professional" means a medical practitioner, dental practitioner, pharmacist, clinical psychologist, nurse, midwife, medical assistant, physiotherapist, occupational therapist and other allied healthcare professionals and any other person involved in the giving of medical, health, dental, pharmaceutical and any other healthcare services under the jurisdiction of the Ministry of Health.

PART IV

EXEMPTION

21. Exemption.

(1) Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes shall be exempted from the provisions of this Act.

(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.

22. Power to make further exemptions.

(1) The Minister may, upon the recommendation of the Information Commissioner, 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

23. Powers of Information Commissioner.

The Information Commissioner shall be the Commissioner appointed pursuant to section 35 of the Freedom of Information Act and he or she 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 his or her functions under this Act.

24. Functions of Information Commissioner.

The functions of the Information Commissioner include–

(a) monitoring compliance by public and private bodies with the provisions 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 of data subjects 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.

PART VI
ENFORCEMENT

25. Receipt and investigation of complaints.

(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 or the Regulations 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.

26. Form of complaint.

(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.

27. Notice of investigation.

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.

28. Information notice.

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

(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.

29. Warrant to enter and search.

(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) 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 or Regulations.

30. Enforcement notice.

(1) Where the Information Commissioner is of the opinion that a public body or a private body has contravened or is contravening a provision of this Act, the contravention of which is an offence, the Information Commissioner may, subject to subsection (2) serve an enforcement notice on the public body or private body, requiring it to take such steps as are specified in the enforcement notice within such time as may be so specified to comply with the provision concerned.

(2) An enforcement notice shall be in writing and shall–

(a) specify the provision of this Act that, in the opinion of the Information Commissioner, the public body or private body has contravened or is contravening and the reasons for the Information Commissioner having formed that opinion; 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, without prejudice to the generality of subsection (2), 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) Where a public body or a private body complies with a requirement under subsection (3), it shall, as soon as practicable and in any event not later than [thirty] days after such compliance, 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 concerned and ending immediately before such compliance;

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

(5) The Information Commissioner may cancel 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.

31. Assessment of processing.

(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 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 Parliament pursuant to this Act.

32. Civil remedies.

(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.

33. Obstruction.

(1) A person shall not obstruct the Information Commissioner or any other authorised officer in the conduct of their duties and functions under this Act.

(2) A person who contravenes this section 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.

34. Whistleblower's protection.

An employer whether or not a public body, shall not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee or deny that employee of 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 described in paragraph (a)

PART VII
OFFENCES

35. Willful disclosure.

(1) A person who wilfully discloses personal information in contravention of this Act, commits an offence.

(2) A person who collects, stores or disposes of personal information in a manner that contravenes this Act, commits an offence.

36. Breach of confidentiality.

A person who breaches the confidentiality obligations established by section 34, commits an offence.

37. Penalties for corporations.

Where a corporation commits an offence under this Act, any officer, director or agent of the corporation who directed, authorised, assented to, or participated in the commission of the offence is a party to and commits an offence and is liable to the punishment provided for the offence.

38. Penalties for offences.

(1) A person who commits an offence under this Act for which a penalty is not specifically provided for is liable upon—

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

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

(2) Where the offences under this Act is committed by a body corporate, the body corporate shall be liable upon—

(a) summary conviction, to a fine of two hundred and fifty thousand dollars; and

(b) conviction on indictment, to a fine of five hundred thousand dollars.

PART VIII
MISCELLANEOUS

39. Appeals to Court.

An appeal lies to the Court against–

(a) a requirement specified in an enforcement notice or an information notice;

(b) a decision of the Information Commissioner in relation to a complaint; or

(c) any decision of the Information Commissioner in respect of the conduct of his or her duties and powers under this Act.

40. Delegations.

The Chief Executive Officer or the Information Commissioner may delegate any power or function under this Act to an authorised officer.

41. Protection from criminal or civil proceedings.

(1) No criminal or civil proceedings shall lie against the Information Commissioner or against a person acting on behalf or under the direction of the Information Commissioner, for anything done, reported or said in good faith in the course of the exercise or performance or purported exercise, discharge, or performance of any power, duty or function of the Information Commissioner under this Act.

(2) For the purpose of the Libel and Slander Act, Cap. 4.18 or 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.

42. Confidentiality.

Subject to this Act, the Information Commissioner and every person acting on behalf 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.

43. Report to Parliament.

(1) The Information Commissioner shall, within three months after the termination of the financial year, prepare a report on the activities of the Information Commissioner as it relates to this Act during that year and cause a copy of the report to be laid before Parliament.

(2) Notwithstanding subsection (1), the Information Commissioner may, at any time, make a special report to Parliament 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 thereon should not be deferred until the time provided for transmission of the next annual report of the Information Commissioner pursuant to subsection (1).

44. Regulations.

(1) The Minister may make Regulations for giving effect to the provisions of this Act and for prescribing anything required or authorised by this Act to be prescribed.

(2) Notwithstanding 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; and

(c) codes of practice.

(3) All Regulations made under this Act shall be laid before Parliament as soon as may be after the making thereof and shall be subject to negative resolution.

AKILAH BYRON-NISBETT

.....
Deputy Speaker

Passed by the National Assembly this 4th day of May, 2018.

SONIA BODDIE-THOMPSON

.....
Clerk of the National Assembly

GOVERNMENT PRINTERY
ST KITTS W I