

SAINT LUCIA

No.11 of 2011

ARRANGEMENT OF SECTIONS

PART I

PRELIMINARY

1. Short title and commencement
2. Interpretation
3. Application
4. State to be bound

PART II

APPOINTMENT, FUNCTIONS AND POWERS OF THE
DATA PROTECTION COMMISSIONER

5. Appointment of Data Protection Commissioner
6. Resources of the office of the Commissioner
7. Restriction on employment
8. Tenure of office
9. Functions of the Commissioner
10. Independence of functions
11. Oath and Confidentiality
12. Powers of the Commissioner
13. Delegation of functions of the Commissioner
14. Power of the Commissioner to obtain information
15. Contents of information notice
16. Failure or refusal to comply with information notice
17. Insufficient information pursuant to the information notice
18. Powers of investigation
19. Form of complaint
20. Notice of investigation
21. Power to request assistance
22. Powers of entry and search
23. Warrant to enter and search premises
24. Obstruction of Commissioner or authorized officer
25. Power of Commissioner to issue enforcement notice
26. Contents of enforcement notice

27. Failure to comply with enforcement notice an offence
28. Investigations in private
29. Referral to Director of Public Prosecutions
30. Instruments of the Commissioner
31. Protection of the Commissioner and staff

PART III

OBLIGATION ON DATA CONTROLLERS

32. Data Protection Principles
33. Collection of personal data
34. Consent for processing of personal data
35. Criteria for processing sensitive personal data
36. Processing of sensitive personal data
37. Processing concerning health or medical purposes
38. Processing and disclosure for research and statistical purposes
39. Processing concerning legal offences
40. Accuracy of personal data
41. Use of personal data
42. Security of personal data
43. Duty to destroy personal data
44. Unlawful disclosure of personal data
45. Transfer of personal data

PART IV

REGISTRATION OF DATA PROTECTION CONTROLLERS

46. Requirement to register
47. Registration as a data controller
48. Duration of registration
49. Register of Data Controllers
50. Inspection of Register
51. Certificate issued by Commissioner

PART V

RIGHTS OF DATA SUBJECTS AND OTHERS

52. Right to access personal data
53. Compliance with request for access to personal data
54. Discretion in relation to access to personal data

- 55. Denial of access to personal data
- 56. Right of rectification, etc. of inaccurate personal data
- 57. Right to prohibit processing of personal data for direct marketing

PART VI

EXEMPTIONS

- 58. National Security
- 59. Crime and taxation
- 60. Health and social work
- 61. Regulatory activities
- 62. Journalism, literature and art
- 63. Research, history and statistics
- 64. Information available to the public under an enactment
- 65. Disclosure required by law or in connection with legal proceedings
- 66. Legal professional privilege
- 67. Domestic purposes
- 68. Written authorization of Commissioner in certain cases

PART VII

MISCELLANEOUS

- 69. Appeals to Court
- 70. Hearing of proceedings
- 71. Offences and penalties
- 72. Offences by directors, etc. of bodies corporate
- 73. Annual Report
- 74. Regulations
- SCHEDULE 1
- SCHEDULE 2

I ASSENT

PEARLETTE LOUISY,
Governor-General.

April 6, 2011.

SAINT LUCIA

No. 11 of 2011

AN ACT to make provision for the protection of individuals in relation to personal data and to regulate the collection, processing, use, and disclosure of personal data in a manner that recognizes the right of privacy of individuals with respect to their personal information and for related matters.

[ON ORDER]

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

PART I
PRELIMINARY

Short title and commencement

1. – (1) This Act may be cited as the Data Protection Act 2011.

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

Interpretation

2. In this Act –

“alternative format” in relation to personal data, means a format that allows a person with a sensory disability to read or listen to the personal data;

“authorized officer” means an officer or employee acting under the direction of the Commissioner or an officer or employee to whom the Commissioner has delegated his or her powers under section 13;

“Caribbean Community” or “Community” means the Caribbean Community established by Article 2 and includes the Caribbean Single Market and Economy (CSME) established by the provisions of the revised CARICOM Treaty;

“Commissioner”-

(a) means the Data Protection Commissioner appointed pursuant to section 5; and

(b) includes an authorized officer of the Commissioner authorized by him or her in that behalf;

“correct” in relation to personal information, means to alter that information by way of correction, deletion, or addition; and “correction” has a corresponding meaning;

“Court” means the High Court or a Judge of the High Court;

“data” includes representations of facts, information or concepts that are being prepared or have been prepared in a form suitable for use in an electronic

system including a computer program, text, image, sound, video and information within a database or electronic system;

“data controller” means a person who, either alone or with others, processes data or determines how personal data are processed or processes personal data;

“Data Protection Principles” includes the principles set out in Schedule 2;

“data subject” means the natural person who is the subject of personal data;

“document”-

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

(b) includes 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 program, or a combination of both, which is used for that purpose by the establishment which holds the record;

“enforcement notice” means a notice issued by the Commissioner under section 25;

“information notice” means a notice issued by the Commissioner under section 14;

“Minister” means the Minister responsible for Information and Broadcasting;

“Permanent Secretary” means the officer for the time being exercising the highest level of administrative functions within any Government Ministry;

“personal data” means information about a data subject that is recorded in any form including -

(a) information relating to the race, national or ethnic origin, religion, age, sexual orientation, sexual life or marital status of the data subject;

(b) information relating to the education, medical, criminal or employment history of the data subject or

information relating to the financial transactions in which the individual has been involved or which refers to the data subject;

- (c) any identifying number, symbol or other particular designated to the data subject;
- (d) the address, fingerprints, Deoxyribonucleic Acid (DNA), or blood type of the data subject;
- (e) the name of the data subject where it appears with other personal data relating to the data subject or where the disclosure of the name itself would reveal information about the data subject;
- (f) correspondence sent to an establishment by the data subject that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence; or
- (g) the views or opinions of any other person about the data subject;

“prescribed” means prescribed by the Regulations made by the Minister;

“processing” in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including-

- (a) organization, adaptation or alteration of the information or data;
- (b) retrieval, consultation or use of the information or data;
- (c) disclosure of the information or data by transmission, dissemination, or otherwise making available; or
- (d) alignment, combination, blocking, erasure or destruction of the information or data;

“public authority” includes any body, for the purposes of this Act-

- (a) established by or under the Constitution;

- (b) established by statute;
- (c) which forms part of any level or branch of Government;
- (d) owned, controlled or substantially financed by funds provided by Government or the State; or
- (e) carrying out a statutory or public authority function:
Except that a body referred to in paragraph (e) is a public authority only to the extent of its statutory or public functions;

“Register” means the Register of Data Controllers required to be kept by the Commissioner pursuant to section 49;

“Regulations” means Regulations made pursuant to section 74;

“relevant person”, in relation to a data subject, means-

- (a) where the data subject is a minor, a person who has parental authority over the minor or has been appointed as his or her guardian by the Court;
- (b) where the data subject is physically and mentally unfit, a person who has been appointed his or her guardian by the Court;
- (c) in any other case, a person duly authorized in writing by the data subject to make a request under section 52;

“sensitive personal data” means personal data consisting of information on a data subject’s-

- (a) racial or ethnic origins;
- (b) political opinions;
- (c) religious beliefs or other beliefs of a similar nature;
- (d) physical or mental health or condition;
- (e) sexual orientation or sexual life; or
- (f) criminal or financial record;

“third party” means a person other than the data subject, the data controller and such other person who under

the direct responsibility of the data controller is authorized to process personal data.

Application

3.—(1) This Act applies to a data controller in respect of any data if —

- (a) the data controller is established in Saint Lucia and the data is processed in the context of the business of that establishment; or
- (b) the data controller is not established in Saint Lucia but uses equipment in Saint Lucia for processing data otherwise than for the purpose of transit through Saint Lucia.

(2) A data controller falling within subsection 1(b) shall nominate for the purposes of this Act a representative established in Saint Lucia.

(3) For the purposes of this section, the following is to be treated as established in Saint Lucia —

- (a) an individual who is ordinarily resident in Saint Lucia or is a national of the Caribbean Community;
- (b) a body incorporated under the Companies Act, Cap 13.01;
- (c) a partnership or other unincorporated association formed under the laws of Saint Lucia; and
- (d) any person who does not fall within paragraphs (a), (b) and (c) but maintains in Saint Lucia an office, branch or agency through which he or she carries on any activity related to data processing.

State to be bound

4. This Act binds the State.

PART II
APPOINTMENT, FUNCTIONS AND POWERS OF THE
DATA PROTECTION COMMISSIONER

Appointment of Data Protection Commissioner

5.—(1) Subject to subsection (2), there shall be a Data Protection Commissioner who shall be appointed in writing by the Governor General acting on the advice of the Prime Minister after the Prime Minister has consulted the Cabinet and the Leader of the Opposition.

(2) A person appointed to be the Data Commissioner under subsection (1) shall be an attorney-at-law within the meaning of the Legal Profession Act, Cap. 2:04, with at least ten years standing at the bar and shall have training or experience in economics, finance, information security, technology, audit or human resource management.

(3) A person shall not be appointed or continue to hold office as Commissioner if that person -

- (a) is a Member of Parliament;
- (b) is a Judge or Magistrate;
- (c) is a member of a local authority;
- (d) has a financial or other interest in any enterprise or activity which is likely to conflict with the discharge of his or her functions as the Commissioner;
- (e) is an undischarged bankrupt; or
- (f) has at any time been convicted of any offence involving dishonesty or moral turpitude.

Resources of the office of the Commissioner

6.—(1) There shall be appointed such officers and employees as may be necessary to enable or assist the Commissioner to discharge the duties and to perform the functions conferred on the Commissioner under this Act effectively and efficiently.

(2) The office of Commissioner must have an independent budget appropriated by Parliament and controlled by the Commissioner.

(3) Parliament shall appropriate annually, for the use of the office of the Commissioner, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Commissioner, of his or her functions, powers and duties under this Act.

Restriction on employment

7. The Commissioner shall not hold any other office of employment in respect of which emoluments are payable.

Tenure of office

8.—(1) The Commissioner shall hold office for a term of five years and is eligible for reappointment on the expiration of his or her term of office.

(2) The Commissioner may resign from office by letter addressed to the Governor General and shall in any case vacate the office of Commissioner on reaching the age of sixty-five years.

(3) The Commissioner may be removed from office only for inability to discharge the functions of his or her office, whether arising from infirmity of body or mind or any other cause, or for misbehaviour.

(4) The Commissioner shall vacate office if any circumstances arise that, if he or she were not Commissioner, would cause him or her to be disqualified for appointment as such by virtue of section 5(3).

(5) Where —

- (a) a vacancy arises in the office of Commissioner; or
- (b) by reason of illness, absence from the country or other sufficient cause, the Commissioner is unable to perform his or her functions under this Act;

the Governor General acting on the advice of the Prime Minister after he or she has consulted the Cabinet and the Leader of the Opposition may appoint a suitable person, to act in that office or perform the functions of the Commissioner, as the case may be.

Functions of the Commissioner**9.** The Commissioner shall –

- (a) create and maintain a register of all data controllers;
- (b) create and maintain a public register of all processing operations according to notifications submitted to him or her as specified in this Act;
- (c) exercise control on all data processing activities and, either of his or her own motion or at the request of a data subject, verify whether the processing of data is carried on in accordance with this Act or the Regulations;
- (d) promote self-regulation among data controllers;
- (e) instruct the data controller to take such measures as may be necessary to ensure that the data processing is undertaken in accordance with this Act or the Regulations;
- (f) receive and investigate reports and claims from data subjects or associations representing the data subject violations of this Act or the Regulations, and take such remedial action as he or she considers necessary or as may be prescribed under this Act, and to inform such data subjects or associations of the outcome;
- (g) issue such directions or public statements as may be required of him or her for the purposes of this Act;
- (h) encourage the drawing up of suitable codes of conduct by the various sectors affected by this Act and ascertain that the provisions of such codes are in accordance with this Act and for such purpose the Commissioner may seek the views of data subjects or their representatives;
- (i) take such measures as may be necessary so as to bring the provisions of this Act to the knowledge of the general public;
- (j) promote by education and publicity, an understanding and acceptance of the data protection principles and of the objects of the principles;

- (k) advise the Government on any legislative measures that are required to be taken in relation to privacy and data protection;
- (l) inquire generally into any matter including an enactment or law or any practice or procedure whether governmental or non-governmental, or any technical development if it appears to the Commissioner that the privacy of data subjects is being or may be infringed;
- (m) examine any legislation that makes provision for the collection of personal data by any public authority or the disclosure of personal data by one public authority to any other public authority and report to the Minister the results of that examination;
- (n) either of his or her own motion or on request, report to the Minister as the need arises on any matter affecting the privacy of a data subject, including any recommendations relating to the need for or the desirability of, taking legislative, administrative or other action to give protection, or better protection, to the privacy of the data subject;
- (o) collaborate with supervisory authorities of other countries to the extent necessary for the performance of his or her functions or duties, in particular by exchanging all useful information, in accordance with any Convention to which Saint Lucia is a party or any other international obligation of Saint Lucia;
- (p) generally monitor compliance by governmental and non-governmental bodies with this Act and the Regulations;
- (q) prepare and issue or approve, in consultation with the Minister, appropriate codes of practice or guidelines for the guidance of business persons and institutions handling personal data;
- (r) undertake research into and monitor developments in data processing and computer technology to ensure that any adverse effects of such developments on the privacy of data subjects are minimized, and include the results of such research and monitoring, if any, in

his or her annual report in accordance with section 73;

- (s) provide advice, with or without request, to a Minister or a public authority on any matter relevant to the operation of this Act and report to the Minister as the need arises on the desirability of the acceptance by Saint Lucia of any international instrument relating to the privacy of data subjects;
- (t) ensure compliance with this Act and the Regulations;
- (u) do any thing incidental or conducive to the performance of any of the preceding functions; and
- (v) exercise and perform such other functions as are conferred or imposed on the Commissioner under this Act, or any other enactment.

Independence of functions

10. In the exercise of his or her functions under this Act the Commissioner shall act independently and is not subject to the direction or control of any other person or authority.

Oath and confidentiality

11. – (1) The Commissioner, and every authorized officer shall take the oath specified in Schedule 1 before the Governor General.

(2) A person who is or has been the Commissioner, an officer of the Commissioner's staff or an agent of the Commissioner shall not make use of or divulge, either directly or indirectly, any data or information obtained as a result of the exercise of a power or in the performance of a duty under this Act, except-

- (a) in accordance with this Act or any other enactment; or
- (b) as authorized by an Order of the Court.

(3) A person who, without lawful excuse, contravenes subsection (2), commits an offence and is liable on summary conviction to a fine not exceeding twenty five thousand dollars or to imprisonment for a term not exceeding six months or to both.

Powers of the Commissioner

12.— (1) The Commissioner shall, for the purpose of carrying out his or her functions do all such acts as appear to him or her to be requisite, advantageous or convenient for, or in connection with the carrying out of his or her functions under this Act.

(2) The Commissioner may, in relation to carrying out of the investigation of any complaint under this Act-

- (a) summon and enforce the appearance of persons before the Commissioner and require the person to give oral or written evidence on oath and to produce such documents and things as the Commissioner considers requisite to the full investigation and consideration of the complaint, in the same manner and to the same extent as a Judge of the High Court;
- (b) administer oaths;
- (c) receive and accept such evidence and other information, whether on oath or by affidavit or otherwise, as the Commissioner sees fit, whether or not the evidence or information is or would be admissible in a Court of law;
- (d) enter any premises occupied by any public authority on satisfying any security requirements of the authority relating to the premises;
- (e) converse in private with any person in any premises entered pursuant to paragraph (d) and otherwise carry out such inquiries within the power of the Commissioner under this Act as the Commissioner sees fit; and
- (f) examine or obtain copies of or extracts from books or other records found in any premises entered pursuant to paragraph (d) containing any matter relevant to the investigation.

(3) The Commissioner may, during the investigation of any complaint under this Act, examine any information recorded in any form held by a public authority and information that the Commissioner may examine under this subsection shall not be withheld from the Commissioner by any person and on any grounds.

(4) Any document or thing produced pursuant to this section by any person or public authority shall be returned by the Commissioner within ten days after a request is made to the Commissioner by that person or authority, but nothing in this subsection precludes the Commissioner from again requiring its production in accordance with this section.

Delegation of functions of the Commissioner

13.— (1) The Commissioner may designate one or more officers or employees under the administrative control of the Commissioner to exercise, discharge or perform any of the power, duties or functions of the Commissioner under this Act, that are specified in the designation.

(2) The Commissioner may delegate any of the investigating and enforcement powers conferred on the Commissioner by this Act to any authorized officer and to any police officer designated for that purpose by the Commissioner of Police.

Power of the Commissioner to obtain information

14.— (1) The Commissioner may, by notice in writing served on any person, request that person to furnish to him or her in writing in the 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 Commissioner of his or her functions and exercise of his or her powers and duties under this Act:

(2) Notwithstanding subsection (1), where the personal data is processed for the purpose of compliance with a legal obligation to which the data controller is subject, the Minister may by Regulation prescribe rules and procedures for the purposes of implementation of this subsection.

(3) Where the information requested by the Commissioner is stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the person named in the information notice shall produce or give access to the information in a form in which it can be taken away and in which it is visible and legible.

(4) A notice required or authorized by this Act to be served on or given to any person by the Commissioner may –

- (a) if that person is an individual, be served on that person at his or her usual or last known address or place of business:
 - (i) by delivering personally to the person;
 - (ii) by sending it to the person by post addressed to him or her; or
 - (iii) by leaving it for the person;
- (b) if that person is a body corporate or partnership, be served:
 - (i) by sending it by post to the proper officer of the body corporate at its principal office;
 - (ii) by addressing it to the proper officer of the partnership and leaving it at the office of the proper officer.

Contents of information notice

15.—(1) Subject to subsection (2), the information notice specified in section 14 must state—

- (a) that the person to whom the notice is addressed has a right of appeal under section 69 against the requirement specified in the notice within thirty days from the service of the notice on him or her; and
- (b) the time for compliance with a requirement specified in the information notice, which time must not be expressed to expire before the end of the period of thirty days specified in paragraph (a).

(2) Where a notice of appeal against a decision made under section 14 is lodged with the Commissioner, the information

required need not be furnished, and section 16 applies pending the determination or withdrawal of the appeal.

(3) If the Commissioner considers that by reason of special circumstances the information is required urgently for the proper performance of his or her functions and exercise of his or her powers under this Act, the Commissioner may apply to a Judge in Chambers for communication of the information.

(4) A law in force in Saint Lucia or rule of law prohibiting or restricting the disclosure of information does not preclude a person from furnishing to the Commissioner any information that is necessary or expedient for the performance by the Commissioner of his or her functions and this subsection does not apply to information that in the opinion of the Minister or the Minister for national security is, or at any time was, kept for the purpose of safeguarding the security of the State or information that is privileged from disclosure in proceedings in any Court.

Failure or refusal to comply with information notice

16.—(1) A person shall not -

- (a) without reasonable excuse, fail or refuse to comply with a requirement specified in an information notice, or
- (b) in purported compliance with an information notice furnish information to the Commissioner that the person knows to be false or misleading in a material respect.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding twenty-five thousand dollars or to a term of imprisonment not exceeding six months or to both.

(3) It is a defence for a person charged with an offence under this section to prove that he or she exercised all due diligence to comply with the information notice.

Insufficient information pursuant to the information notice

17. If the Commissioner cannot, pursuant to a request under section 14(1), obtain sufficient information in order to conclude that the processing of personal data is lawful, the Commissioner may prohibit the data controller from processing personal data in any other manner than by storing the personal data.

Powers of investigation

18. — (1) The Commissioner may 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 data controller in relation to a data subject if -

- (a) the data subject complains to the Commissioner of a contravention of this Act, or
- (b) the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act.

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

- (a) investigate the complaint or cause it to be investigated by an authorized officer, unless he or she is of the opinion that it is frivolous or vexatious; and
- (b) as soon as reasonably practicable, notify the data subject concerned in writing of his or her decision in relation to the complaint and that the data subject may, if aggrieved by the decision of the Commissioner appeal against the decision to the Court under section 69.

(3) This Act does not preclude the Commissioner from receiving and investigating complaints that are submitted by a person authorized in writing by the data subject concerned, to act on behalf of that data subject, and a reference to a data subject in any other section of this Act includes a reference to a person so authorized.

Form of complaint

19. — (1) A complaint pursuant to this Act must be made to the Commissioner in writing unless the Commissioner authorizes otherwise.

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

Notice of investigation

20. Before commencing an investigation of a complaint pursuant to this Act, the Commissioner shall notify, in the case of a public authority, the Permanent Secretary, and in any other case the person responsible for the administration or management of the public authority or establishment, of the intention to carry out the investigation and shall include in the notification the substance of the matter under investigation.

Power to request assistance

21. — (1) For the purposes of gathering information or for the proper conduct of any investigation concerning compliance with this Act, the Commissioner may seek the assistance of such persons or authorities, as the Commissioner thinks fit and that person or authority may do such things as are reasonably necessary to assist the Commissioner in the performance of the Commissioner's functions.

(2) Any person assisting the Commissioner pursuant to subsection (1), shall for the purpose of section 13 be deemed to be an authorized officer.

Powers of entry and search

22. — (1) Subject to subsection (2), the Commissioner or an authorized officer who is accompanied by a police officer may at any time enter any premises, for the purpose of discharging any functions or duties under this Act or the Regulations only on production of a warrant issued by a Magistrate under section 23.

(2) An authorized officer shall not enter any premises unless he or she is accompanied by a police officer and shows to the owner or occupier of the premises a warrant issued by a Magistrate under section 23.

Warrant to enter and search premises

23.—(1) If a Magistrate is satisfied by information on oath supplied by the Commissioner or an authorized officer that there are reasonable grounds for suspecting that:

- (a) a data controller has contravened or is contravening any of the data protection principles; or
- (b) an offence under this Act has been or is being committed,

and that evidence of the contravention or of the commission of the offence is to be found on any premises specified by the Commissioner or an authorized officer, the Magistrate may issue a warrant authorizing the entry and search of the premises.

(2) A warrant issued under subsection (1) must authorize a police officer accompanied by the Commissioner or an authorized officer at all reasonable times within seven days of the date of the warrant to enter the premises to -

- (a) request the owner or occupier to produce any document, record or data;
- (b) examine any document, record or data and take copies or extracts from the document record or data;
- (c) inspect, examine, operate and test any data equipment found on the premises;
- (d) request the owner of the premises entered into, or any person employed by him or her, or any other person on the premises, to give to the authorized officer all reasonable assistance and to answer all reasonable questions either orally or in writing.

(3) The police officer shall at the time of execution of the warrant, show the warrant and supply a copy of the warrant to the person who owns or occupies the premises in respect of which a warrant is issued.

(4) The Commissioner or an authorized officer shall provide an inventory of the type of data collected or seized to the data controller or the owner or occupier of premises who supplies the data to the Commissioner or the authorized officer.

Obstruction of Commissioner or authorized officer

24.—(1) A person shall not obstruct or impede the Commissioner, an authorized officer or any other person acting on behalf or under the direction of the Commissioner in the discharge and performance of the duties and functions conferred on the Commissioner by this Act.

(2) A person who contravenes subsection (1) commits an offence and is liable, on summary conviction, to a fine not exceeding twenty-five thousand dollars or to a term of imprisonment not exceeding six months or to both.

Power of Commissioner to issue enforcement notice

25.—(1) If the Commissioner is of the opinion that a data controller has contravened or is contravening a provision of this Act, other than a provision the contravention of which is an offence, the Commissioner may, by an enforcement notice in writing served on the data controller, require the data controller to take such steps as are specified in the enforcement notice within such time, as is specified in the enforcement notice, to comply with the relevant provision.

(2) Without prejudice to the generality of subsection (1), if the Commissioner is of the opinion that a data controller has contravened a Data Protection Principle, the Commissioner may issue an enforcement notice requiring the data controller to -

- (a) rectify or erase any of the data concerned; or
- (b) supplement the data with such statement relating to the matters dealt with by the data controller as the Commissioner may approve.

(3) A data controller who, as required under subsection (2)(b), supplements data that is inaccurate or not kept up to date, is not deemed to be in contravention of the Data Protection Principles.

Contents of enforcement notice

26.—(1) An enforcement notice issued by the Commissioner under section 25 must -

- (a) specify any provision of this Act that, in the opinion of the Commissioner, the data controller has contravened or is contravening and the reasons for the Commissioner having formed that opinion; and
- (b) subject to subsection (2), inform the data subject of his or her right to appeal to the Court under section 69 against the requirement specified in the notice within thirty days from the service of the notice on him or her.

(2) Subject to subsection (3), the time specified in an enforcement notice for compliance with a requirement specified in the enforcement notice shall not be expressed to expire before the end of the period of thirty days specified in subsection (1) (b) and, if an appeal is brought against the requirement, the requirement need not be complied with, pending the determination or withdrawal of the appeal.

(3) If the Commissioner -

- (a) by reason of special circumstances, is of the opinion that a requirement specified in an enforcement notice must be complied with urgently; and
- (b) such enforcement notice includes a statement to that effect,

subsections (1) (b) and (2) do not apply in relation to the notice, but the notice must contain a statement of the right of appeal of the applicant under section 69, and must not require compliance with the requirement before the end of the period of seven days beginning on the date on which the notice is served.

(4) On compliance by a data controller with a requirement under subsection (2) of section 25, the data controller shall, as soon as may be and in any event not more than thirty days after such compliance, notify -

- (a) the data subject concerned; and
- (b) any person, where the Commissioner considers it reasonably practicable to do so, to whom the data were disclosed during the period beginning twelve months before the date of the service of the enforcement notice concerned and ending immediately before such compliance, of the rectification, erasure or statement

concerned, if such compliance materially modifies the data concerned.

(5) The Commissioner may cancel an enforcement notice and, if he or she does so, shall notify in writing the person on whom it was served accordingly.

Failure to comply with enforcement notice an offence

27.—(1) A person shall not, without reasonable excuse, fail or refuse to comply with a requirement specified in an enforcement notice.

(2) A person who contravenes subsection (1) commits an offence and is liable, on summary conviction, to a fine not exceeding twenty-five thousand dollars or to a term of imprisonment not exceeding six months or to both.

Investigations in private

28.—(1) All deliberations or hearings in relation to an investigation under this Act may be conducted in private.

(2) In the course of a deliberation or hearing in relation to an investigation under this Act by the Commissioner, the person who made the complaint and the Permanent Secretary or the person responsible for the administration of the public authority or in any other case, the chief executive officer of the entity or establishment concerned, shall be given an opportunity to make representations to the Commissioner, but none is entitled as of right to be present during representations made to the Commissioner by any other person.

Referral to Director of Public Prosecutions

29. On completion of an investigation under this Act, the Commissioner shall, where the investigation reveals that an offence has been committed under this Act or any regulations made under this Act, refer the matter to the Director of Public Prosecutions for necessary action.

Instruments of the Commissioner

30. Any document purporting to be an instrument made, issued, or signed by the Commissioner must be received in

evidence and must, until the contrary is proved, be deemed to be an instrument made, issued or signed by the Commissioner.

Protection of the Commissioner and staff

31. An action or other proceedings for damages must not be instituted against the Commissioner, or against any person acting on behalf or under the direction of the Commissioner, for anything done, reported or said in good faith in the exercise of a discretion or in the discharge or performance of any power, duty or function of the Commissioner under this Act.

PART III

OBLIGATION ON DATA CONTROLLERS

Data Protection Principles

32. The data controller shall comply with the Data Protection Principles set out in Schedule 2, in relation to all personal data processed by the data controller.

Collection of personal data

33. – (1) Subject to Part VI, a data controller shall not collect personal data unless –

- (a) the data is collected for a lawful purpose connected with a function or activity of the data controller; and
- (b) the collection of the data is necessary for that purpose.

(2) Where a data controller collects personal data directly from a data subject, the data controller shall at the time of collecting the personal data ensure that the data subject concerned is informed of -

- (a) the fact that the personal data is being collected;
- (b) the purpose for which the personal data is being collected;
- (c) the intended recipients of the personal data;
- (d) the name and address of the data controller;
- (e) whether or not the supply of the personal data by that data subject is voluntary or mandatory;

- (f) the consequences for that data subject if all or any part of the requested personal data is not provided;
- (g) whether or not the data collected will be further processed and whether or not the consent of the data subject would be required for the further processing; and
- (h) the data subject's right of access to, the possibility of correction of and destruction of, the personal data to be provided.

(3) A data controller shall not be required to comply with subsection (2):

- (a) in respect of a data subject where-
 - (i) compliance with subsection (2) in respect of a second or subsequent collection will be to repeat, without any material difference, what was done to comply with that subsection in respect of the first collection; and
 - (ii) not more than twelve months have elapsed between the first collection and the second or subsequent collection.
- (b) where:
 - (i) compliance is not reasonably practicable at the time of collection, provided that the data controller makes available to the data subject all the relevant information specified in subsection (2) as soon as practicable; or
 - (ii) the personal data is used in a form in which the data subject concerned cannot or could not reasonably expect to be identified.

(4) Where personal data is not collected directly from the data subject concerned, the data controller or any person acting on his or her behalf shall ensure that the data subject is informed of the matters specified in subsection (2).

(5) Subsection (3) does not operate to prevent a second or subsequent collection from becoming a first collection where

the data controller has complied with subsection (2) in respect of the second or subsequent collection.

Consent for processing of personal data

34.—(1) Subject to subsection (2), a data controller shall not process personal data unless the data controller has obtained the express consent of the data subject.

(2) Notwithstanding subsection (1), a data controller may process personal data without obtaining the express consent of the data subject where the processing is necessary -

- (a) for the performance of a contract to which the data subject is a party;
- (b) in order to take steps required by the data subject prior to entering into a contract;
- (c) in order to protect the vital interests of the data subject;
- (d) for compliance with any legal obligation to which the data controller is subject;
- (e) for the administration of justice;
- (f) for the performance of an activity that is carried out in the public interest or in the exercise of official authority vested in the data controller or in a third party to whom the personal data is disclosed;
- (g) for a purpose that concerns a legitimate interest of the data controller or of such a third party to whom personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject and in particular the right to privacy.

(3) Where the data controller processes personal data under paragraphs (f) and (g) of subsection (2), the data subject shall, except where otherwise provided in any other law in force in Saint Lucia, be entitled to object at any time to the data controller on compelling legitimate grounds to the processing of the personal data.

(4) Where the data controller processes personal data with the consent of the data subject, the data subject may at any

time revoke his or her consent for compelling legitimate grounds relating to his or her particular situation.

(5) A data controller who contravenes this section commits an offence and is liable on summary conviction to a fine not exceeding twenty-five thousand dollars or to imprisonment for a term not exceeding six months.

Criteria for processing sensitive personal data

- 35.** A person shall not process sensitive personal data –
- (a) except in cases provided for-
 - (i) in subsection (2) of section 34 or sections 36, 37 and 38;
 - (ii) in regulations prescribed by the Minister having regard to the public interest; or
 - (b) unless the data subject-
 - (i) has given his or her explicit consent to the processing; or
 - (ii) has published the personal data.

Processing of sensitive personal data

36. The data controller may process sensitive personal data if appropriate safeguards are adopted and the processing is necessary -

- (a) for the purposes of exercising or performing any right or obligation which is conferred or imposed by any law in force in Saint Lucia on the data controller;
- (b) in order to protect the vital interests of the data subject or another person in a case where-
 - (i) consent cannot physically or legally be given by or on behalf of the data subject; or
 - (ii) the data controller cannot reasonably be expected to obtain the consent of the data subject;
- (c) 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.

Processing concerning health or medical purposes

37.—(1) Sensitive personal data may be processed for health and hospital care purposes, if the sensitive personal data is processed by a health practitioner or other person subject to the obligation of professional confidentiality and the processing is necessary for-

- (a) preventive medicine and the protection of public health;
- (b) medical diagnosis;
- (c) health care or treatment; or
- (d) management of health and hospital care services.

(2) For the purposes of subsection (1) “health practitioner” means a person who is registered pursuant to the Health Practitioners Act, 2006 No. 33.

Processing and disclosure for research and statistical purposes

38.—(1) A data controller may process or disclose sensitive personal data or may cause sensitive personal data in his or her custody or control to be processed or disclosed for a research purpose, including statistical research only if -

- (a) the research purpose cannot reasonably be accomplished unless that data is provided in individually identifiable form;
- (b) the data is disclosed or processed on condition that the data is not to be used for the purpose of contacting a person to participate in research;
- (c) any record linkage is not harmful to the data subject and the benefits to be derived from the record linkage are clearly in the public interest;
- (d) the disclosure or processing is necessary for the purposes stipulated in section 34(2)(f);
- (e) the person responsible for the administration of the public authority or in any other case, the chief executive officer of the establishment concerned, has approved conditions relating to the following:
 - (i) security and confidentiality;
 - (ii) the removal or destruction of the individual identifiers at the earliest reasonable time;

- (iii) the prohibition of any subsequent use or disclosure of that data in individually identifiable form without the express authorization of the public authority or establishment concerned; and
- (f) the person to whom the sensitive personal data is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public authority's or establishment's policies and procedures relating to the confidentiality of personal data.

(2) Personal data may be provided to be used for the purposes referred to in subsection (1), unless otherwise provided by applicable rules on secrecy and confidentiality.

Processing concerning legal offences

39.—(1) Data relating to offences, criminal convictions or security measures may only be processed under the control of a public authority.

(2) The Minister may by regulations authorize any person to process the data referred to in subsection (1), subject to such suitable specific safeguards as may be prescribed.

(3) A complete register of criminal convictions may only be kept under the control of a public authority.

Accuracy of personal data

40. A data controller shall take all reasonable steps to ensure that personal data in his or her possession —

- (a) remains accurate; and
- (b) is kept up-to-date where such personal data requires regular updating.

Use of personal data

41. A data controller shall ensure that personal data is —

- (a) kept only for one or more specified and lawful purposes for which the personal data is to be processed;

- (b) not used or disclosed in any manner incompatible with the purposes for which the personal data has been processed;
- (c) adequate and relevant for the purpose for which the personal data is to be processed; and
- (d) not kept for longer than is necessary for the purpose for which the personal data is to be processed.

Security of personal data

42. – (1) A data controller shall –

- (a) take appropriate security and organizational measures for the prevention of unauthorized access to, alteration of, disclosure of, accidental loss, and destruction of the personal data in the data controller's control; and
- (b) ensure that the measures provide a level of security appropriate to –
 - (i) the special risks that exist in the processing of the personal data; and
 - (ii) the nature of the personal data being processed.

(2) A data controller shall take all reasonable steps to ensure that any person employed by the data controller is aware of and complies with the relevant security measures referred to in subsection (1).

(3) Without prejudice to subsection (1), in determining the appropriate security measures, in particular, where the processing involves the transmission of personal data over an information and communication network, a data controller shall have regard to –

- (a) the state of technological development available; and
- (b) the cost of implementing any of the security measures.

Duty to destroy personal data

43. Where the purpose for keeping personal data has lapsed, the data controller shall destroy the personal data and render the personal data inaccessible as soon as reasonably practicable, in accordance with the Regulations.

Unlawful disclosure of personal data

44.—(1) A data controller shall not without lawful authority disclose personal data in any manner that is incompatible with the purposes for which the personal data has been collected.

(2) A person, other an employee or agent of a data controller acting within his or her mandate, shall not —

- (a) obtain access to personal data, or obtain any information constituting such personal data, without the prior authority of the data controller by whom the personal data is kept; and
- (b) disclose the personal data or information to another person.

(3) A person shall not offer to sell personal data where that personal data has been obtained in contravention of this section.

(4) For the purposes of subsection (3) an advertisement indicating that personal data is or may be for sale, constitutes an offer to sell the personal data.

(5) A person who contravenes this section commits an offence and is liable on summary conviction to a fine not exceeding twenty-five thousand dollars or to a term of imprisonment not exceeding six months or to both.

Transfer of personal data

45.—(1) Subject to subsection (2), a data controller shall not transfer personal data to a country or territory outside Saint Lucia unless —

- (a) the country or territory to which the personal data is being transferred has comparable safeguards to those in Saint Lucia for the protection of the rights and freedom of the data subject in relation to the processing of personal data; and
- (b) the Commissioner has authorized the data controller to transfer the personal data to the country or territory outside Saint Lucia.

(2) Subsection (1)(a) does not apply if —

- (a) the data subject has given his or her consent to the transfer;
- (b) the transfer is necessary -
 - (i) for the performance of a contract between the data subject and the data controller, or for the taking of steps at the request of the data subject with a view to entering into a contract with the data controller;
 - (ii) for the conclusion of a contract between the data controller and a person, other than the data subject, which is entered at the request of the data subject, or is in the interest of the data subject for the performance of such a contract; or
 - (iii) to safeguard national security or where section 56 applies;
- (c) the matter concerns public security; or
- (d) the transfer is made on such terms as may be approved by the Commissioner as ensuring the adequate safeguards for the protection of the rights of the data subject.

PART IV

REGISTRATION OF DATA PROTECTION CONTROLLERS

Requirement to register

46.—(1) A person shall not process personal data as a data controller unless that person is registered as a data controller is made in accordance with section 47.

(2) A person, who without reasonable excuse processes any personal data without being registered under this Act commits an offence and is liable on summary conviction to a fine not exceeding twenty-five thousand dollars or to a term of imprisonment not exceeding six months or to both.

Registration as a data controller

47.—(1) An application for registration as a data controller must be made in writing to the Commissioner and the person shall furnish the particulars required under section 49(a), (c), (d),(e) and (f).

(2) Subject to subsection (3), the Commissioner shall grant an application for registration, unless the Commissioner reasonably believes that -

- (a) the particulars proposed for inclusion in an entry in the register are insufficient or any other information required by the Commissioner either has not been furnished, or is insufficient;
- (b) appropriate safeguards for the protection of the privacy of the data subjects concerned are not being, or will not continue to be, provided by the data controller; or
- (c) the person applying for registration is not a fit and proper person in the determination of the Commissioner.

(3) On registration as a data controller, the applicant shall pay the prescribed fee.

(4) Where the Commissioner refuses an application for registration, the Commissioner shall, as soon as reasonably practicable notify, in writing, the applicant of the refusal -

- (a) specifying the reasons for the refusal; and
- (b) informing the applicant that he or she may appeal against the refusal under section 69.

Duration of registration

48.—(1) A registration under this Part is for a period not exceeding twelve months and on the expiry of such period, the relevant entry must be cancelled unless the registration is renewed.

(2) The period specified under subsection (1) is calculated -

- (a) in the case of a first registration, from the date on which the relevant entry was made in the register; and
- (b) in the case of a registration which has been renewed, from the date on which registration was renewed.

(3) The Commissioner may register an applicant for a period shorter than twelve months if, on examining the application,

the Commissioner determines that the shorter period is adequate for the processing of the data in respect of which the application is made.

(4) The Commissioner may renew a registration on application by the data controller, and on payment of the prescribed fee.

Register of Data Controllers

49. The Commissioner shall keep a register to be known as the Register of Data Controllers in which he or she shall cause to be entered in relation to each data controller, the following particulars:

- (a) the name and address;
- (b) the date of registration;
- (c) a description of the personal data processed by the data controller and of the categories of data subjects to which they relate;
- (d) a description of the purpose for which the personal data is processed;
- (e) a description of any recipient or recipients to whom the data controller intends or may wish to disclose the personal data; and
- (f) the names, or a description of, any countries or territories outside the Caribbean Community the State to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the personal data.

Inspection of Register

50.— (1) The Register of Data Controllers shall be kept in the office of the Commissioner and shall at all reasonable times be available for inspection by any person free of charge.

(2) A person may, on payment of the prescribed fee, obtain from the Commissioner a certified copy of, or a certified copy of an extract from any entry in the Register.

Certificate issued by Commissioner

51. In any proceedings in which the registration of a person as a data controller is in question, a certificate under the hand of the Commissioner that there is no entry in the Register in respect of the person as a data controller, is proof in the absence or evidence to the contrary of that fact.

PART V
RIGHTS OF DATA SUBJECTS AND OTHERS

Right to access personal data

52. – (1) This section applies to a person who has reasonable grounds to believe that he or she is the subject of personal data that has been or is being processed by a particular data controller.

(2) A data controller shall on the written request of a data subject or a relevant person –

- (a) provide a written response to the data subject or the relevant person setting out the following –
 - (i) whether the data kept by the data controller includes personal data relating to the data subject or the relevant person;
 - (ii) a description of that personal data, if any;
 - (iii) the purposes for which the personal data are being or are to be processed;
 - (iv) the source from which the information is being collected;
 - (v) the logic that is involved in any automatic processing of personal data concerning the data subject or the relevant person;
 - (vi) the recipients or classes of recipients to whom they are or may be disclosed; and
- (b) permit the data subject or the relevant person to examine the personal data in accordance with the regulations or supply the data subject or the relevant person with a copy of any personal data referred to in paragraph (a) on payment of the prescribed fee.

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

- (a) the personal data already exists in an alternative format that is acceptable to the data subject or relevant person; or
- (b) the data controller considers it to be reasonable to cause the personal data to be converted.

(3) Where any personal data referred to under subsection (1) is expressed in terms that are not intelligible without explanation, the data controller shall supply the information with an explanation of the terms.

(4) The information to be supplied pursuant to a request under this section must be supplied by reference to any personal data at the time when the request is received, except that it may take account of any amendment or deletion made between that time and the time when the information is supplied.

Compliance with request for access to personal data

53.—(1) Subject to this section and section 54 and to the payment of the prescribed fee, a data controller shall comply with a request under section 52 not later than thirty days after the receipt of the request.

(2) Where a data controller is unable to comply with the request within the period specified in subsection (1), the data controller shall before the expiry of the specified period –

- (a) inform the data subject or the relevant person who has made the request on behalf of the data subject, that the data controller is unable to comply with the request and shall if required state the reasons for the data controller's inability to comply; and
- (b) obtain an extension of time from the data subject or relevant person or endeavour to comply with the request in such time as may be mutually agreed between the data subject or relevant person and the data controller.

(3) If the parties do not, within forty-eight hours of the data subject or relevant person being informed under paragraph (2)(a), agree to an extension of the thirty days, the data controller shall apply to the Commissioner without delay, and the Commissioner shall, without delay, fix a new deadline for compliance.

Discretion in relation to access to personal data

54. – (1) A data controller may refuse to comply with a request made under section 52 where –

- (a) the data controller is not supplied with such information as the data controller may reasonably require in order to satisfy the data controller as to the identity of the person making the request, and to locate the information which the person seeks; or
- (b) compliance with such request will be in contravention with his or her confidentiality obligation imposed under this Act or any other enactment.

(2) Where a data controller cannot comply with a request made under section 52 without disclosing personal data relating to another person, the data controller may refuse the request unless -

- (a) the other individual has consented to the disclosure of his or her personal data to the person making the request; or
- (b) the data controller obtains the written approval of the Commissioner.

(3) In determining for the purposes of subsection (2) (b) whether it is reasonable for the Commissioner to approve a request without the consent of the other individual concerned, regard must be had, in particular, to -

- (a) any duty of confidentiality owed to the other individual;
- (b) any steps taken by the data controller with a view to seeking the consent of the other individual;
- (c) whether the other individual is capable of giving consent; and
- (d) any express refusal of consent by the other individual.

(4) Where a data controller has previously complied with a request made under section 52 by a data subject or relevant person, the data controller is not obliged to comply with a subsequent identical or similar request under section 52 by that data subject or relevant person unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(5) In determining, for the purposes of subsection (4), whether request under section 52 are made at reasonable intervals, regard must be had to –

- (a) the nature of the data;
- (b) the purpose for which the data is processed; and
- (c) the frequency with which the data is altered.

Denial of access to personal data

55.—(1) A data controller shall not comply with a request under section 52 where –

- (a) he or she is being requested to disclose information given or to be given in confidence for the purposes of –
 - (i) the education, training or employment, or prospective education, training or employment, of the data subject;
 - (ii) the appointment, or prospective appointment, of the data subject to any office; or
 - (iii) the provision, or prospective provision, by the data subject of any service;
- (b) the personal data requested consist of information recorded by candidates during an academic, professional or other examination;
- (c) such compliance would, by revealing evidence of the commission of any offence other than an offence under this Act, expose him or her to proceedings for that offence.

(2) The data controller shall notify the data subject or relevant person, in writing, of a refusal of a request made by a data subject or relevant person and shall include a statement of

the reasons for the refusal and an indication that the data subject or relevant person may complain to the Commissioner about the refusal.

Right of rectification, etc. of inaccurate personal data

56.—(1) Where personal data processed by a data controller to which access has been given under any enactment, contains personal data of a data subject which the data subject claims:

- (a) is incomplete, incorrect, misleading, or excessive;
- (b) not relevant to the purpose for which the data is held;

the data controller shall, on application of the data subject, cause such data to be rectified, blocked, erased, destroyed or annotated as appropriate.

(2) Where a data controller has permitted a third party to have access to personal data referred to in subsection (1), he or she shall, as soon as reasonably practicable, request the third party to rectify, block, erase, destroy or annotate the data, as appropriate.

(3) Where a data controller or a third party fails to rectify, block, erase or destroy personal data referred to in subsection (1) (a) and (b), a data subject may apply to the Commissioner to have such data rectified, blocked, erased, destroyed, rendered inaccessible or annotated as appropriate.

(4) On being satisfied by an application under subsection (3) that the personal data is the data referred to in subsection (1) (a) and (b), the Commissioner shall direct the data controller to rectify, block, erase, destroy render inaccessible or annotate the data and any other personal data in respect of which he or she is the data controller.

(5) The Commissioner may direct the data controller to notify third parties to whom data has been disclosed, of any rectification, blocking, erasure, destruction or annotation of the data, if the Commissioner —

- (a) issues a direction under subsection (4); or
- (b) is satisfied on the application by an individual that personal data of which the individual is the data subject

were inaccurate and have been rectified, blocked, erased, destroyed or annotated.

(6) The data controller shall comply with a direction issued under this section within fourteen days of receipt of the direction.

Right to prohibit processing of personal data for direct marketing

57. – (1) A person may, at any time, by notice in writing, request a data controller –

- (a) to stop; or
- (b) not to begin,

the processing of personal data in respect of which he or she is a data subject, for the purposes of direct marketing.

(2) Where the data controller receives a request under subsection (1) (a), he or she shall, without delay and in any event not more than thirty days after the request has been received, where the personal data are kept -

- (a) only for purposes of direct marketing, erase the data; and
- (b) for direct marketing and other purposes, stop processing the personal data for direct marketing.

(3) Where the data controller receives a request under subsection (1) (b), the data controller -

- (a) shall, where the personal data are kept only for the purpose of direct marketing, as soon as reasonably practicable and in any event not more than thirty days after the request has been received, erase the personal data; or
- (b) shall not, where the personal data are kept for direct marketing and other purposes, process the personal data for direct marketing after the expiry of thirty days.

(4) The data controller shall notify the data subject in writing of any action taken under subsections (2) and (3) and, where appropriate, inform the data subject of the other purposes for which the personal data is being processed.

(5) Where a data controller fails to comply with a notice issued pursuant to subsection (1), the data subject may make a complaint to the Commissioner.

(6) In this section, “direct marketing” means a communication, by whatever means, of any advertising or marketing material which is directed to particular individuals.

PART VI EXEMPTIONS

National Security

58. The Minister may by Order exempt a data controller from complying with any provision of this Act if the Minister determines that such non-compliance is required to safeguard national security.

Crime and taxation

59. A data controller which is a public authority is exempt from:

- (a) the Second, Third, Fourth and Eighth Data Protection Principles specified in Schedule 2;
- (b) sections 34, 35, 40, 41, and 45; and
- (c) Part V in respect of blocking personal data, to the extent to which the application of such provisions would be likely to prejudice any of the matters specified in this section;
- (d) if the processing of personal data is required for the purposes of -
 - (i) the prevention or detection of crime;
 - (ii) the apprehension or prosecution of offenders; or
 - (iii) the assessment or collection of any tax, duty or any imposition of a similar nature.

Health and social work

60.—(1) A data controller is exempt from the application of section 52 where the personal data to which access is being sought relates to the physical or mental health of the data subject

or any relevant person and the application of that section is likely to cause serious harm to the physical or mental health of the data subject or of any relevant person.

(2) The Minister may, by Order published in the *Gazette* waive the obligations imposed under section 52, on a public authority, voluntary organizations and any other similar body as may be prescribed, where the public authority, voluntary organization or other body carries out social work in relation to a data subject or any other individual, and the application of that section is likely to prejudice the carrying out of the social work.

Regulatory activities

61.— (1) This section applies to the processing of personal data by a data controller for the purposes of discharging any of the relevant functions —

- (a) designed for protecting members of the public against -
 - (i) financial loss due to dishonesty, malpractice or other serious improper conduct, or by the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate;
 - (ii) financial loss due to the conduct of discharged or undischarged bankrupts; or
 - (iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorized to carry on any profession or other activity;
- (b) conferred on the Eastern Caribbean Central Bank, the Director of Financial Services and the Financial Intelligence Unit, by or under any enactment;
- (c) for protecting charitable trusts and other bodies involved in charitable work against misconduct or mismanagement in administration;
- (d) for protecting the property of charitable trusts and other bodies specified in paragraph (c) from loss or misapplication;

- (e) for the recovery of the property of charitable trusts and other bodies specified in paragraph (c);
- (f) for securing the health, safety and welfare of persons at work;
- (g) for protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work; or
- (h) designed for –
 - (i) protecting members of the public against conduct which adversely affect their interests by persons carrying on a business;
 - (ii) regulating agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity; or
 - (iii) regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market.

(2) The processing of personal data by a data controller for the purpose of discharging any of the relevant functions referred to in subsection (1) (a) to (h), is exempt from the application of sections 34, 35, 40, 41 and 45 to the extent that the application of these sections would be likely to prejudice the proper discharge of the relevant functions.

Journalism, literature and art

62. – (1) The processing of personal data for journalistic, literary and artistic purposes is exempt from the provisions specified in subsection (2) where –

- (a) such processing is undertaken with a view to the publication of any journalistic, literary or artistic material;
- (b) the data controller involved in such processing reasonably believes that the publication would be in the public interest; and

- (c) the data controller reasonably believes that compliance with any such provisions would be incompatible with such purposes.

(2) For the purposes of subsection (1), the processing of personal data is be exempt from –

- (a) the Second, Fourth and Eighth Data Protection Principles and the part of the Third Data Protection Principle which states that personal data must be relevant and not excessive in relation to the purposes for which they are to be processed;
- (b) sections 34, 35, 40, 41, and 45; and
- (c) Part IV in respect of blocking personal data.

Research, history and statistics

63.—(1) Subject to subsections (2), (4), and (5), personal data which is processed only for research, historical or statistical purposes is be exempt from the Fourth Data Protection Principle.

(2) The exemption provided for under subsection (1) is not applicable where –

- (a) the personal data is not processed to support measures or decisions with respect to particular individuals; and
- (b) the personal data is not processed in such a way that such processing would substantially damage or substantially distress any data subject or will likely cause such damage or distress.

(3) For the purposes of –

- (a) the Second Data Protection Principle; and
- (b) sections 34, 35, 40 and 41, further processing of personal data only for research, historical or statistical purposes is not regarded as incompatible with the purposes for which such data was obtained provided that the conditions under subsection (2) are satisfied.

(4) The personal data processed for research, historical or statistical purposes is also exempt from the provisions of Part V where -

- (a) the conditions under subsection (2)(a) and (b) are satisfied; and
- (b) the results of the research or any resulting statistics are not made available in a form which identifies any of the data subjects concerned.

Information available to the public under an enactment

64. Where personal data consists of information that the data controller is obliged under an enactment to make available to the public, such data is exempt from -

- (a) the Second, Third, Fourth and Eighth Data Protection Principles;
- (b) sections 34, 35, 40, 41, 42, 43 and 44; and
- (c) Part V in respect of blocking personal data.

Disclosure required by law or in connection with legal proceedings

65. The disclosure of personal data by a data controller is exempt from -

- (a) the Second, Third, and Fourth Data Protection Principles;
- (b) sections 34, 35, 40, 41, 42, 43 and 44; and
- (c) Part V in respect of blocking personal data;
- (d) if the disclosure of the personal data is -
 - (i) required under any enactment or by a Court order;
 - (ii) necessary for the purpose of, or in connection with, any on-going or prospective legal proceedings;
 - (iii) necessary for the purpose of obtaining legal advice; or
 - (iv) otherwise necessary for the purpose of establishing, exercising or defending legal rights.

Legal professional privilege

66. Personal data is exempt from –

- (a) the Second, Third, and Fourth Data Protection Principles; and
- (b) section 40, where the personal data consist of information in respect of which a claim to legal professional privilege or confidentiality as between client and legal practitioner could be maintained in legal proceedings, including prospective legal proceedings.

Domestic purposes

67. Where personal data is processed by an individual only for the purposes of that individual's personal, family or household affairs or for recreational purposes, the personal data is exempt from –

- (a) the Data Protection Principles; and
- (b) Parts IV and Part V.

Written authorization of Commissioner in certain cases

68. The investigations on the data processing described in Part VI are subject to the written authorization of the Commissioner.

PART VII
MISCELLANEOUS

Appeals to Court

69. – (1) An appeal may be made to and heard and determined by the Court against –

- (a) a requirement specified in an enforcement notice or an information notice;
- (b) a decision of the Commissioner in relation to a complaint; or
- (c) any decision of the Commissioner in respect of the performance of his or her duties and powers under this Act.

(2) An appeal must be brought within thirty days from the service on the person concerned of the relevant notice, or, as the case may be, the receipt by such person of the notification of the relevant refusal or decision.

(3) Where –

- (a) a person appeals to the Court pursuant to paragraph (a), (b) or (c) of subsection (1);
- (b) the appeal is brought within the period specified in the notice; and
- (c) the Commissioner has included a statement in the relevant notice or notification to the effect that by reason of special circumstances he or she is of opinion that the requirement or prohibition specified in the notice should be complied with, or the refusal specified in the notification should take effect urgently;

the Court may determine on application made to it in that behalf, that non-compliance by the person with a requirement or prohibition specified in the notice during the period ending with the determination of withdrawal of the appeal or during such other period as may be determined by the Court does not constitute an offence.

Hearing of proceedings

70. The whole or any part of any proceedings under this Act may, at the discretion of the Court, be heard otherwise than in public.

Offences and penalties

71. – (1) A person who contravenes this Act commits an offence.

(2) If a specific penalty is not provided for an offence, the person is liable –

- (a) in the case of an individual, to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding six months or to both;
- (b) in the case of a body corporate, to a fine not exceeding one hundred thousand dollars.

Offences by directors, etc. of bodies corporate

72. If any provision of this Act is contravened by a body corporate and the contravention is proved to have been done with the consent or connivance of or to be attributable to any neglect on the part of any individual, being a director, manager, secretary or other officer of that body corporate, or an individual who was purporting to act in any such capacity that individual, as well as the body corporate, commits an offence and is liable:

- (a) in the case of the individual, to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding six months, or to both.
- (b) in the case of the body corporate, to a fine not exceeding one hundred thousand dollars.

Annual Report

73.—(1) The Commissioner shall as soon as practicable after the thirty-first day of December of each year, prepare an annual report on the activities of the office of Commissioner and cause a copy of the report to be laid before the Parliament no later than 31 March in each subsequent year.

(2) Without limiting the generality of subsection (1), the report must include —

- (a) a statement about the operation of approved and issued codes of practice;
- (b) any recommendation that the Commissioner thinks fit relating to the compliance with this Act, and in particular the Data Protection Principles.

Regulations

74.—(1) The Minister may, after consultation with the Commissioner, make Regulations for giving effect to the purpose 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) rules and procedures relating to access by the Commissioner of data held in instances where the data controller processes data for compliance with a legal obligation;
- (b) guidelines for the disposal of personal data held by a data controller;
- (c) guidelines for the contents of any notifications or applications made pursuant to this Act;
- (d) the fees that may be levied by the Commissioner;
- (e) the extension of the application of this Act to any particular activity or sector;
- (f) the issuing and approval of codes and guidelines; and
- (g) guidelines and rules relating to the provisions of this Act.

(3) All Regulations made under this Act are subject to negative resolution of Parliament.

SCHEDULE 1

Section 11

FORM OF OATH

(AFFIRMATION FOR DATA PROTECTION COMMISSIONER)

I.....,make oath/solemnly affirm/
declare that I will faithfully and honestly fulfill my duties as authorized
officer/Commissioner in conformity with the Data Protection Act 2010
and without fear or favour affection or ill-will and that I shall not without
the due authority in that behalf disclose or make known any matter or
thing which comes to my knowledge by reason of my duties as
Commission, authorized officer, employee.

SCHEDULE 2

Section 32(1)

DATA PROTECTION PRINCIPLES

- (a) First Principle - Collection Limitation Principle: Personal data shall be processed fairly and lawfully in accordance with section 33.
- (b) Second Principle - Purpose Specification Principle: Personal data shall be obtained only for one or more specified and lawful purposes, which purpose shall be specified not later than at the time of data collection, and such personal data shall not be further processed in any manner incompatible with that purpose or those purposes in accordance with sections 33 and 41.
- (c) Third Principle - Data Quality Principle: Personal data shall be relevant and not excessive in relation to the purposes for which they are to be processed and, to the extent necessary for those purposes, shall be accurate, complete and up-to-date in accordance with sections 40 and 41.
- (d) Fourth Principle - Use Limitation Principle: Personal data shall not be disclosed, made available or otherwise used for purposes other than those specified under this Act and such personal data processed for any purpose shall not be kept longer than is necessary for that purpose or those purposes in accordance with sections 41, 42 and 44.
- (e) Fifth Principle - Security Safeguard Principle: Personal data shall be protected by reasonable security safeguards and appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against such risks as accidental loss, unauthorized access, use, modification, or destruction of data in accordance with section 33.
- (f) Sixth Principle - Accountability Principle: A data controller shall be accountable for complying with measures which give effect to the data protection principles and shall ensure that personal data is processed in accordance with the rights of the data subject under this Act in accordance with section 33.
- (g) Seventh Principle - Individual Participation Principle: A data subject shall have the right to know what data is held about him by a data controller and shall have a right to ensure that all reasonable measures are taken to complete, correct, block, erase or annotate data to the extent that such data is incomplete or incorrect, having

regard to the purposes for which they are processed in accordance with sections 33 and 56.

- (h) Eighth Principle – Transfer of Data Principle: Personal data shall not be transferred to a country or territory outside the State unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data in accordance with section 45.

Passed in the House of Assembly this 22nd day of March, 2011.

ROSEMARIE HUSBANDS-MATHURIN,
Speaker of the House.

Passed in the Senate this 24th day of March, 2011.

EVERISTUS JN. MARIE
Deputy President of the Senate.

