

OBJECTS AND REASONS

This Bill would provide for

- (a) the regulation of the collection, keeping, processing, use or dissemination of personal data;
- (b) the protection of the privacy of individuals in relation to personal data; and
- (c) related matters **related thereto**.

Arrangement of Sections

Section

PART I

Preliminary

1. Short title.
2. Interpretation.
3. Application of Act.

PART II

DATA PROTECTION PRINCIPLES

4. Data protection principles.
5. The interpretation of the first data protection principle.
6. The application of the first data protection principle.
7. Processing of sensitive personal data.
8. The application of the second data protection principle.
9. The application of the fourth data protection principle.
10. The application of the sixth data protection principle.
11. The application of the seventh data protection principle.
12. The application of the eighth data protection principle.

PART III

THE DATA PROTECTION COMMISSIONER

Establishment, Functions and Powers

13. Establishment of the Commissioner.
14. Functions of the Commissioner.
15. Protection of the Commissioner.
16. Confidentiality.

PART IV

RIGHTS OF DATA SUBJECTS AND OTHERS

17. Right of access to personal data.
18. Application of section 17 where data controller is a credit reference agency.
19. Right to prevent processing likely to cause damage or distress.
20. Right to prevent processing of indirect marketing.
21. Rights in relation to automated decision making.
22. Compensation for failure to comply with certain requirements.
23. Rectification, blocking, erasure and destruction.

PART V

REGISTRATION OF DATA CONTROLLERS

24. Data Controllers must be registered.
25. Register of Data Controllers.
26. Notification of changes.

Section

PART VI

EXEMPTIONS

27. References.
28. National Security.

29. Crime and taxation.
30. Health, education and social work.
31. Regulatory activity.
32. Research, history and statistics.
33. Information available to the public by or under enactment.
34. Disclosures required by law or made in connection with legal proceedings etc.
35. Legal professional privilege.
36. Domestic purposes.
37. Powers to make further exemptions by Order.

PART VII

ENFORCEMENT

38. Enforcement notice.
39. Cancellation of enforcement notice.
40. Request for assessment.
41. Information notices.
42. Failure to comply with notice.
43. Service of notice by the Commissioner.

Section

44. Warrants.
45. Execution of warrants.
46. Matters exempt from inspection and seizure.
47. Return of warrants.
48. Obstruction of execution of a warrant.

PART VIII

DATA PROTECTION TRIBUNAL

- 49. Establishment of the Data Protection Appeal Tribunal.
- 50. Rights of appeal.
- 51. Determination of appeals.

PART IX

MISCELLANEOUS

- 52. Unlawful obtaining etc. of personal data.
- 53. Disclosure of information.
- 54. Liability of directors, etc.
- 55. Act binds Crown.
- 56. Regulations.
- 57. Commencement.

FIRST SCHEDULE

SECOND SCHEDULE

OBJECTS AND REASONS

This Bill would provide for

- (a) the regulation of the collection, keeping, processing, use or dissemination of personal data;
- (b) the protection of the privacy of individuals in relation to personal data; and
- (c) related matters **related thereto**.

Arrangement of Sections

Section

PART I

Preliminary

1. Short title.
2. Interpretation.
3. Application of Act.

PART II

DATA PROTECTION PRINCIPLES

4. Data protection principles.
5. The interpretation of the first data protection principle.
6. The application of the first data protection principle.
7. Processing of sensitive personal data.
8. The application of the second data protection principle.
9. The application of the fourth data protection principle.
10. The application of the sixth data protection principle.
11. The application of the seventh data protection principle.
12. The application of the eighth data protection principle.

Section

PART III

THE DATA PROTECTION COMMISSIONER

Establishment, Functions and Powers

13. Establishment of the Commissioner.
14. Functions of the Commissioner.
15. Protection of the Commissioner.
16. Confidentiality.

PART IV

RIGHTS OF DATA SUBJECTS AND OTHERS

17. Right of access to personal data.
18. Application of section 17 where data controller is a credit reference agency.
19. Right to prevent processing likely to cause damage or distress.
20. Right to prevent processing of indirect marketing.
21. Rights in relation to automated decision making.
22. Compensation for failure to comply with certain requirements.
23. Rectification, blocking, erasure and destruction.

PART V

REGISTRATION OF DATA CONTROLLERS

24. Data Controllers must be registered.
25. Register of Data Controllers.
26. Notification of changes.

Section

PART VI

EXEMPTIONS

27. References.
28. National Security.

29. Crime and taxation.
30. Health, education and social work.
31. Regulatory activity.
32. Research, history and statistics.
33. Information available to the public by or under enactment.
34. Disclosures required by law or made in connection with legal proceedings etc.
35. Legal professional privilege.
36. Domestic purposes.
37. Powers to make further exemptions by Order.

PART VII

ENFORCEMENT

38. Enforcement notice.
39. Cancellation of enforcement notice.
40. Request for assessment.
41. Information notices.
42. Failure to comply with notice.
43. Service of notice by the Commissioner.

Section

44. Warrants.
45. Execution of warrants.
46. Matters exempt from inspection and seizure.
47. Return of warrants.
48. Obstruction of execution of a warrant.

PART VIII

DATA PROTECTION TRIBUNAL

- 49. Establishment of the Data Protection Appeal Tribunal.
- 50. Rights of appeal.
- 51. Determination of appeals.

PART IX

MISCELLANEOUS

- 52. Unlawful obtaining etc. of personal data.
- 53. Disclosure of information.
- 54. Liability of directors, etc.
- 55. Act binds Crown.
- 56. Regulations.
- 57. Commencement.

FIRST SCHEDULE

SECOND SCHEDULE

BARBADOS

A Bill entitled

An Act to provide for

- (a) the regulation of the collection, keeping, processing, use or dissemination of personal data;
- (b) the protection of the privacy of individuals in relation to personal data; and
- (c) related matters **related thereto**.

ENACTED by the Parliament of Barbados as follows:

PART I

Preliminary

1. This Act may be cited as the *Data Protection Act, 2005*.
2. In this Act,

"accessible public record" means any record that is kept by any authority to which members of the public are given access;

"accessible record" means

- (a) a health record;
- (b) an educational record; or
- (c) an accessible public record;

"credit reference agency" means a person carrying on a business comprising the furnishing of persons with information relevant to the financial standing of individuals, being information collected by the agency for that purpose;

"Commissioner" means Data Protection Commissioner;

"data" means information that

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

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

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or

(d) does not fall within paragraphs (a), (b) or (c) but forms part of an accessible record;

"data controller" means a person who determines the purposes for which and the manner in which any personal data is processed;

"data processor" in relation to personal data, means any person other than an employee of the data controller who processes the data on behalf of the data controller;

"data subject" means an individual who is the subject of personal data;

"personal data" means data which relates to an individual who can be identified

(a) from that data; or

(b) from other information which is in the possession of or is likely to come into the possession of the data controller;

"processing" in relation to information and data, means obtaining, recording or holding information or data or carrying out any operation or set of operations on the information and 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;

"Register" means the Register of Data Controllers required to be kept by the Data Protection Commissioner under section 25;

"relevant filing system" means any set of information or data relating

to individuals to the extent that although the information or data is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that the specific information or data relating to a particular individuals is readily accessible;

"sensitive personal data" means personal data consisting of information on a data subject's

- (a) racial or ethnic origin;
- (b) political opinions;
- (c) religious beliefs or other beliefs of a similar nature;
- [(d) membership of any organization whether [social,] economic or otherwise;]
- (e) physical or mental health or condition;
- (f) sexual orientation or sexual life;
- (g) criminal or financial record; or
- (h) proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

3. (1) Except as otherwise provided herein, this Act applies to a data controller in respect of any data if

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

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

(3) For the purposes of this section, each of the following is to be treated as established in Barbados:

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

PART II

DATA PROTECTION PRINCIPLES

4. (1) There shall be data protection principles with which a data controller shall comply in relation to all personal data processed by the data controller.

(2) The data protection principles referred to under subsection (1) are as follows:

- (a) **First Principle:** personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless there is compliance with at least one of the conditions set out in
 - (i) section 6; and
 - (ii) in the case of sensitive personal data, section 7;
- (b) **Second Principle:** personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- (c) **Third Principle:** personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- (d) **Fourth Principle:** personal data shall be accurate and, where necessary, kept up-to-date;
- (e) **Fifth Principle:** personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;

- (f) **Sixth Principle:** personal data shall be processed in accordance with the rights of data subjects under this Act;
- (g) **Seventh Principle:** appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data; and
- (h) **Eighth Principle:** personal data shall not be transferred to a country or territory outside Barbados 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.

(3) Any person who fails to comply with the data protection principles is guilty of an offence and is liable on indictment to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.

5. (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(2) Subject to subsection (3), for the purposes of the first principle, data are to be treated as having been obtained fairly if they consist of information obtained from a person who

- (a) is authorised by or under any enactment to supply it; or
- (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on Barbados.

(3) For the purposes of the first principle personal data are not to be treated as processed fairly unless

- (a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the following information:
 - (i) the identity of the data controller;
 - (ii) the identity of that representative, where a data controller has nominated a representative for the purposes of this

Act;

- (iii) the purpose or purposes for which the data are intended to be processed; and
- (iv) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair; and

(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraphs (i) to (iv) of paragraph (a);

(4) For the purposes of paragraph (b) of subsection (3), "the relevant time" means

- (a) the time when the data controller first processes the data; or
- (b) in a case where at that time disclosure to a third party within a reasonable period is envisaged,
 - (i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed;
 - (ii) if within that period the data controller becomes, or ought to become aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware; or

(iii) in any other case, the end of that period.

6. (1) The data controller shall for the purposes of the first principle process personal data only where the data subject has given his consent in writing to the processing **and the the processing is necessary**

- (a) for the performance of a contract to which the data subject is a party; or
- (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 controller is subject, other than an obligation imposed by contract;

- (d) in order to protect the vital interests of the data subject;
- (e) for the administration of justice;
- (f) for the exercise of any functions conferred on any person by or under any enactment;
- [(g) for the exercise of any functions of the **government** or a Minister of **government**;
- (h) **for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject; and**
- (i) for the exercise of any other functions of a public nature exercised in the public interest by any person.

(2) The Minister may by Order specify particular circumstances in which this subsection is or is not taken to be satisfied.

7. (1) The data controller shall not process sensitive personal data unless the data subject has given his consent in writing **and the processing**

- (a) is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
- (b) is necessary in order to protect the vital interests of the data subject or another person, in a case where
 - (i) consent cannot 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; or
- (c) is necessary 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;
- (d) is carried out in the course of its legitimate activities by any body or association which
 - (i) is not established or conducted for profit; and

- (ii) exists for political, philosophical, religious or trade-union purposes;
- (e) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
- (f) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes;
- (g) does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (h) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
- (i) the purpose of obtaining legal advice;
- (j) the purposes of establishing, exercising or defending legal rights;
- (k) the administration of justice;
- (l) the exercise of any functions conferred on any person by or under an enactment;
- (m) the exercise of any functions of the Crown, a Minister of the Crown or a government department;
- (n) is necessary for medical purposes and is undertaken by
 - (i) a health professional;
 - (ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional;
 - (iii) in this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services;
- (o) is of sensitive personal data consisting of information as to racial or ethnic origin;
- (p) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between

persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
(q) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

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

8. (1) For the purposes of the application of the second data protection principle the purpose for which personal data are obtained shall be specified

(a) in a notice given by the data controller to the data subject; or

(b) in a notification given to the Commissioner under Part IV of this Act.

(2) In determining whether any disclosure of personal data is compatible with the purpose for which the data were obtained, regard is to be had to the purpose for which the personal data are intended to be processed by any person to whom they are disclosed.

9. The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where

(a) having regard to the purpose for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and

(b) if the data subject has notified the data controller of the data subject's view that the data is inaccurate and the data indicates that fact.

10. A person is to be regarded as contravening the sixth principle if, but only if he contravenes

(a) section 17 by failing to supply information in accordance with that section;

(b) section 19 by failing to comply with a notice given under subsection (1) of that section to the extent that the

- notice is justified or by failing to give a notice under subsection (3) of that section;
- (c) section 20 by failing to comply with a notice given under subsection (1) of that section; or
 - (d) section 21 by failing to comply with a notice given under subsection (1) or (2) of that section or by failing to give a notification under subsection (3) of that section or a notice under subsection (4) of that section.

11. For the purposes of the application of the seventh data protection principle and having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to

- (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle; and
- (b) the nature of the data to be protected.

(2) The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

(3) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle

- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- (b) take reasonable steps to ensure compliance with those measures.

(4) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless

- (a) the processing is carried out under a contract
 - (i) which is made or evidenced in writing; and
 - (ii) under which the data processor is to act only on

instructions from the data controller; and

- (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

12. (1) For the purposes of the application of the eighth data protection principle, an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to

- (a) the nature of the personal data;
- (b) the country or territory of origin of the information contained in the data;
- (c) the country or territory of final destination of that information;
- (d) the purposes for which and period during which the data are intended to be processed;
- (e) the law in force in the country or territory in question;
- (f) the international obligations of that country or territory;
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory whether generally or by arrangement in particular cases; and
- (h) any security measures taken in respect of the data in that country or territory.

(2) The eighth data protection principle shall not apply where

- (a) the data subject has given his consent to the transfer;
- (b) the transfer is necessary for
 - (i) the performance of a contract between the data subject and the data controller;
 - (ii) the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller;
 - (iii) the conclusion of a contract between the data controller and a person other than the data subject

which

- (A) is entered into at the request of the data subject; or
 - (B) is in the interests of the data subject;
 - (iv) the performance of a contract under paragraph (b)(iii);
 - (v) reasons of substantial public interest;
 - (vi) the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (vii) the purpose of obtaining legal advice;
 - (viii) the purposes of establishing, exercising or defending legal rights; or
 - (ix) the protection of the vital interests of the data subject;
- (c) the transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer;
- (d) the transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; or
- (e) the transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.
- (3) The Minister may by Order specify
- (a) circumstances in which a transfer is to be taken for the purposes of **subsection (1)** to be necessary for reasons of substantial public interest; and
 - (b) circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purpose of **subsection (1)** to be necessary for reasons of substantial public interest.

PART III

THE DATA PROTECTION COMMISSIONER

Establishment, Functions and Powers

13. (1) There shall be a Commissioner called the Data Protection Commissioner, who shall be appointed in the manner set out in the *First Schedule*.

(2) The *First Schedule* has effect with respect to the Commissioner and otherwise in relation thereto.

14. The functions of the Commissioner are to

- (a) promote, by education and publicity, an understanding and acceptance of the data protection principles and of the objects of those principles;
- (b) when requested to do so by a person or agency, conduct an audit of personal data maintained by that person or agency for the purpose of ascertaining whether or not the information is maintained according to the data protection principles;
- (c) monitor the use of personal data and sensitive personal data, and to report to the Minister from time to time on the results of that monitoring, including any recommendations relating to the need for, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the privacy of a person;
- (d) examine any proposed legislation that makes provisions for
 - (i) the collection of personal data by any public sector agency; or
 - (ii) the disclosure of personal data by one public sector agency to any other public sector agencyand report to the responsible Minister the results of that examination;
- (e) receive and invite representations from members of the public on any matter affecting the privacy of a person;
- (f) consult and co-operate with other persons and bodies concerned with the privacy of a person;
- (g) make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that

- person in the interests of the privacy of a person;
- (h) provide advice, with or without a request, to a Minister or an agency on any matter relevant to the operation of this Act;
 - (i) inquire generally into any matter, including any enactment, 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 a person is being or may be infringed thereby;
 - (j) undertake research into, and to monitor developments in data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons are minimised, and to report to the Minister the results of such research and monitoring;
 - (k) examine any proposed legislation or proposed policy of the Government that the Commissioner considers may affect the privacy of persons, and to report to the Minister the results of that examination;
 - (l) report, with or without request, to the Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of a person;
 - (m) report to the Minister from time to time on the desirability of the acceptance, by Barbados, of any international instrument relating to the privacy of the person and advise on the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of a person;
 - (n) prepare appropriate codes of practice for the guidance of business persons and institutions handling personal data;
 - (o) investigate complaints from persons concerning abuses in the use of personal data;
 - (p) do anything incidental or conducive to the performance of any of the preceding functions; and
 - (q) exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

15. No action or other proceeding for damages shall be instituted against a Commissioner for an act done in good faith in the

performance of a duty or in the exercise of a power under this Act.

16. (1) No person who is or who has been the Commissioner, a member of the Commissioner's staff or an agent of the Commissioner shall make use, either directly or indirectly, of any information obtained as a result of his performance of his duties or otherwise for his own benefit or advantage.

(2) No person who is or who has been the Commissioner, a member of the Commissioner's staff or an agent of the Commissioner shall disclose any information which

- (a) has been obtained by or furnished to the Commissioner under or for the purposes of this Act;
- (b) relates to an identified or identifiable person or business; and
- (c) is not at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.

(3) For the purposes of subsection (2) a disclosure of information is made with lawful authority only if and to the extent that

- (a) the disclosure is made with the consent of the individual or of the person for the time being carrying on the business;
- (b) the information was provided for the purpose of its being made available to the public under any provision of this Act;
- (c) the disclosure is made for the purposes of and is necessary for, the discharge of any function under this Act;
- (d) the disclosure is made for the purposes of any proceedings, whether criminal or civil and whether arising under or by virtue of this Act or otherwise; or
- (e) having regard to the rights and freedoms or legitimate interests of any person, the disclosure is necessary in the public interest.

(4) Any person who contravenes subsections (1) or (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 and to imprisonment for 6 months.

PART IV

RIGHTS OF DATA SUBJECTS AND OTHERS

17. (1) Subject to the provisions of this Act, a person has the right
- (a) to be informed by the data controller whether the personal data of which that person is the data subject is being processed by or on behalf of the data controller;
 - (b) where personal data of the data subject is being processed by or on behalf of the data controller, to request the data controller to supply the data subject with a description of
 - (i) the personal data of which that person is the data subject;
 - (ii) the purposes for which the personal data is processed;
 - (iii) the recipients or classes of recipients to whom they are or may be disclosed; and
 - (iv) where processing by automatic means of sensitive personal data of the data subject for the purpose of evaluating matters related to him and is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in the decision taking.
 - (c) to have communicated to the data subject in an intelligible form
 - (i) information constituting any personal data of the data subject; and
 - (ii) any information available to the data controller as to the source of that data.
- (2) A data controller is not obliged to supply any information under subsection (1) unless the data controller has received
- (a) a request in writing; and
 - (b) such fee as the Minister may prescribe.
- (3) A data controller is not obliged to comply with a request under this section unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the data subject making the request and to locate the information that the data subject seeks.

(4) Where a data controller cannot comply with the request under this section without disclosing information relating to a third party who can be identified from that information, the data controller is not obliged to comply with the request unless

- (a) the third party has consented to the disclosure of the information to the data subject making the request; and
- (b) it is reasonable in all the circumstances to comply with the request without the consent of the third party.

(5) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the third party concerned, regard shall be had, in particular to

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

(6) Where a data controller refuses to comply with a request under this section he shall give reasons in writing for his refusal.

(7) A person aggrieved by the decision of the data controller may appeal to the Commissioner.

(8) Subject to subsection (4), a data controller shall comply with a request under this section within 30 days of the date of receipt of that request.

18. (1) Where the data controller is a credit reference agency, section 9 has effect subject to the provisions of this section.

(2) A person making a request under section 17 may limit his request to personal data relevant to his financial standing, and shall be taken to have so limited his request unless the request shows a contrary intention.

(3) Where the data controller receives a request under section 17 in a case where personal data of which the person making the request is the data subject is being processed by or on behalf of the data controller, the obligation to supply information under that section includes an obligation to give the person making the request a

statement, in such a form as may be prescribed by the Minister, of the person's rights.

19. (1) Subject to subsection (2), a data subject is entitled to require the data controller at the end of a 21 day period by notice in writing, to cease, or not begin processing or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the grounds that,

- (a) the processing of that data or the data controller's processing for that purpose or in that manner is causing or is likely to cause substantial damage or distress to the data subject or another; and
- (b) damage or distress is or would be unwarranted.

(2) Subsection (1) does not apply

- (a) in a case where any of the conditions in paragraphs 1(a) to (b)(iv) of section 6(1); or
- (b) in such other cases as may be prescribed by the Minister by Order.

(3) The data controller shall within 21 days of receiving a notice under subsection (1) give the data subject written notice

- (a) stating that he has complied or intends to comply with the data subject's notice;
- (b) stating reasons for his refusal to comply with a data subject's notice; or
- (c) stating the reasons for complying with part of the data subject's notice and the extent of that compliance.

(4) If a court is satisfied, on the application of any data subject who has given notice under subsection (1), that the data controller in question has failed to comply with the notice, the court may order the data controller to take such steps for complying with that notice as the court sees fit.

20. (1) A data subject is entitled at any time by notice in writing to a data controller to require the data controller at the end of a 21 day period to cease, processing for the purposes of direct marketing personal data in respect of which he is the data subject.

(2) If a court is satisfied, on the application of data subject who has given notice under subsection (1), that the data controller has failed to comply with the notice, the court may order data controller to take such steps for complying with the notice as the court sees fit.

(3) For the purposes of this section "indirect marketing" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

21. (1) An **individual** is entitled at any time, by notice in writing to a data controller, to require the data controller to ensure that no decision is taken by or on behalf of the data which significantly affects that **individual** and is based solely on processing by automatic means of sensitive personal data for the purpose of evaluating matters related to the **individual**

(2) A data controller shall inform a data subject by notice of any decision made by the data controller or on the half of the data controller which is made solely on the processing by automatic means of sensitive personal data for the purpose of evaluating any matters related to that data subject.

(3) The data subject is entitled, within 21 days of receiving that notification from the data controller under subsection (2), by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.

(4) The data controller shall within 21 days of receiving a notice under subsection (3) give the individual a written notice specifying the steps that the data controller intends to take to comply with the data subject's notice.

(5) A notice under subsection (1) does not have effect in relation to an exempt decision; and nothing in subsection (2) applies to an exempt decision.

(6) For the purposes of this section "exempt decision" means any decision

- (a) in respect of which the conditions in subsections (7) and (8) are met; or
- (b) which is made in such other circumstances as may be prescribed by the Minister.

(7) The condition in this subsection is that the decision

(a) is taken in the course of steps taken

- (i) for the purpose of considering whether to enter into a contract with the data subject;

- (ii) with a view to entering into such contract;
- (iii) in the course of performing such a contract; or
- (b) is authorised or required by or under any enactment.
- (8) The condition in this subsection is that either
 - (a) the effect of the decision is to grant a request of the data subject; or
 - (b) steps have now been taken to safeguard the legitimate interests of the data subject.

(9) If a court is satisfied, on the application of the data subject that a data controller taking a decision in respect of that data subject has failed to comply with subsection (1) or subsection (2), the court may order the data controller to reconsider the decision, or to take a new decision which is not based solely on processing by automatic means.

22. (1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress where

- (a) the individual also suffers damage by reason of the contravention; or
- (b) the contravention relates to the processing of personal data for
 - (i) the purposes of journalism;
 - (ii) artistic purposes; or
 - (iii) literary purposes.

(3) In proceedings brought against a person by virtue of this section it is a defence to prove that the data controller had taken such care as all the circumstances reasonably required to comply with the requirements concerned.

23. (1) Where a court is satisfied on the application of a data subject that personal data of which the applicant is the subject is inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contains an expression of opinion which appears to the court to be based on the inaccurate data.

(2) Subsection (1) applies whether or not the data accurately records information received or obtained by the data controller from the data subject or a third party but where the data accurately records such information, where

- (a) the requirements mentioned in section 9 have been complied with, the court may, instead of making an order under subsection (1), make an order requiring the data to be supplemented by such statement of the true facts relating to the matters dealt with by the data as the court may approve; and
- (b) all or any of those requirements have not been complied with, the court may, instead of making an order under that subsection, make such order as it thinks fit for securing compliance with those requirements with or without a further order requiring the data to be supplemented by such a statement as is mentioned in paragraph (a).

(3) Where the court

- (a) makes an order under subsection (1); or
- (b) is satisfied on the application of a data subject that personal data of which he was the data subject and which have been rectified, blocked, erased or destroyed were inaccurate,

it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.

(4) Where a court is satisfied on the application of a data subject

- (a) that he has suffered damage by reason of any contravention by a data controller of any of the requirements of this Act in respect of any personal data, in circumstances entitling him to compensation under section 22; and
- (b) that there is a substantial risk of further contravention in

respect of those data in such circumstances,
the court may order the rectification, blocking, erasure or destruction of any of those data.

(5) Where the court makes an order under subsection (4) it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.

(6) In determining whether it is reasonably practicable to require such notification as is mentioned in subsection (3) or (5) the court shall have regard, in particular, to the number of persons who would have to be notified.

PART V

REGISTRATION OF DATA CONTROLLERS

24. (1) A person shall not operate as a data controller unless he is registered in the Register of Data Controllers, maintained by the Commissioner and referred to in section 25.

(2) A person who desires to operate as a data controller may

(a) on making an application to the Commissioner in the form prescribed by the Minister; and

(b) on payment to the Commissioner of the prescribed fee

obtain a certificate from the Commissioner for that purpose.

(3) A person who operates without being registered in the manner described under this section shall be liable on summary conviction to pay a fine of \$5 000 or to a term of imprisonment of 2 months or to both.

25. (1) The Commissioner shall keep a register to be known as the Register of Data Controllers in which he shall cause to be entered in relation to the data controller, the following particulars:

(a) the name and address;

(b) the date of registration;

(c) a description of the personal data processed by or on behalf of the data controller and of the category or categories of data subject to which they relate;

- (d) a description of the purpose or purposes for which the data is processed;
- (e) a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data; and
- (f) the names, or a description of, any countries or territories outside the Caribbean Community to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data.

(2) The Register shall at all reasonable times be open to inspection at the Office **of the Commissioner**.

(3) The Commissioner shall make all amendments to the Register as are necessary.

26. (1) The data controller has a duty to notify the Commissioner of any changes which may affect the particulars entered by the Commissioner in the Register.

(2) A data controller who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$1 000 or to imprisonment for a term of **3 months** and the Commissioner may remove that data controller from the Register.

(3) On receiving notification of the data controller under subsection (1) the Commissioner shall make such amendments to the Register as are necessary.

PART VI

EXEMPTIONS

27. (1) In this Part "the subject information provisions" means

- (a) the first data protection principle to the extent to which it requires compliance with section 5(2); and
- (b) section 17.

(2) In this part "the non-disclosure provisions" means

- (a) the first data protection principle, except to the extent to which it requires compliance with section 6 and section 7;
- (b) the second, third, fourth and fifth data protection principles under section 4; and

(c) sections 19 and 23(1) to (3)

to the extent to which they are inconsistent with the disclosure in question.

(3) Except as provided by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorizing the withholding of information.

28. (1) Personal data is exempt from

(a) section 5;

(b) Parts IV and V; and

(c) section 52

where the exemption from **those provisions** is required for the purpose of safeguarding national security.

29. (1) Personal data processed for

(a) the prevention or detection of crime;

(b) the apprehension or prosecution of offenders; or

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

is exempt from the first data protection principle, except to the extent to which it requires compliance with the conditions in section 6, section 7 and section 17 in any case to the extent to which the application of those provisions to the data is likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data which

(a) is processed for the purpose of discharging statutory functions; and

(b) consists of information obtained for such a purpose from a person who had it in his possession for any of the purposes under subsection (1)

is exempt from the subject information provisions to the same extent as personal data processed for any of the purposes under subsection (1).

(3) Personal data is exempt from the non-disclosure provisions in any case in which

- (a) the disclosure is for any of the purpose under subsection (1); and
 - (b) the application of those provisions in relation to disclosure is likely to prejudice any of the matters mentioned under subsection (1).
- (4) Personal data in respect of which the data controller is a government department, which
- (a) consist of a classification applied to the data subject as a part of a system of risk assessment which is operated by the relevant authority for
 - (i) the assessment or collection of any tax, duty or of any imposition of a similar nature; or
 - (ii) the prevention or detection of crime, or apprehension or prosecution of offenders, where the offence involves any unlawful claim for payment out of or any unlawful application of public funds; and
 - (b) is processed for either of those purposes

is exempt from section 17 to the extent to which the exemption is required in the interests of the operation of the system.

30. (1) The Minister may by Order exempt from the subject information provisions, or modify those provisions in relation to personal data

- (a) consisting of information as to the physical or mental health or condition of a data subject;
- (b) in respect of which the data controller is an educational institution within the meaning assigned to it under section 2 of the *Education Act*, and which consists of information relating to persons who are or have been pupils at the educational institution;
- (c) in respect of which the data controller is a tertiary institution within the meaning assigned to it under section 2 of the *Education Act*, and which consists of information relating to persons who are or have been students at the tertiary institution;

- (d) of other descriptions as may be specified in the Order, being information processed
 - (i) by government departments, public service, charities or other entities designated by or under the Order; and
 - (ii) in the course of, or for the purposes of carrying out social work in relation to the data subject

to the extent that the Minister is satisfied that the carrying out of social work is likely to be prejudiced.

31. (1) Personal data processed for the purposes of discharging functions to which this subsection applies is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is designed for the purpose of

- (a) protecting members of the public against
 - (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or 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 authorised to carry on any profession or other activity;
- (b) protecting charities against misconduct or mismanagement, whether by trustees or other persons in their administration;
- (c) protecting the property of charities from loss or misapplication;
- (d) the recovery of the property of charities;
- (e) securing the health, safety and welfare of persons at work; or

(f) 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.

(3) In subsection (2) "relevant function" means

(a) any function conferred on any person by or under any enactment;

(b) any function of a Minister or government department; or

(c) any other function which is of a public nature and is exercised in the public interest.

(4) Personal data processed for the purpose of discharging any function which is designed for protecting members of the public against

(a) maladministration by public bodies;

(b) failure in services provided by public bodies; or

(c) a failure of a public body to provide a service which is a function of the body to provide

is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data is likely to prejudice the proper discharge of that function.

(5) Personal data processed for the purpose of discharging any function which is designed for

(a) protecting members of the public against conduct which may adversely affect their interests by persons carrying on a business;

(b) 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

(c) regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market

is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

32. (1) In this section

"research purposes" includes statistical or historical purposes;

"the relevant conditions", in relation to any processing of personal data, means the conditions

- (a) that the data are not processed to support measures or decisions with respect to particular individuals; and
- (b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be caused to any data subject.

(2) For the purposes of the second data protection principle under section 5, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(3) Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle under section 5, be kept indefinitely.

(4) Personal data which are processed only for research purposes is exempt from section 17 if

- (a) they are processed in compliance with the relevant conditions; and
- (b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

(5) For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed

- (a) to any person, for research purposes only;
- (b) to the data subject or a person acting on his behalf;
- (c) at the request, or with the consent, of the data subject or a person acting on his behalf; or
- (d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c).

33. Personal data are exempt from

- (a) the subject information provisions;
- (b) the fourth data protection principle under section 5 and section 22(1) to (3); and
- (c) the non-disclosure provisions

if the data consist of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

34. (1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

- (2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary
 - (a) for the purpose of, or in connection with, any legal proceedings including prospective legal proceedings; or
 - (b) for the purpose of obtaining legal advice

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

35. Personal data is exempt from the subject information provisions if the data consists of information in respect of which a claim to legal professional privilege applies.

36. Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs including recreational purposes is exempt from the data protection principles under section 5 and the provisions of Parts IV and V.

37. (1) The Minister may by Order exempt from the subject information provisions personal data consisting of information the disclosure of which is prohibited or restricted by or under any enactment if and to the extent that he considers it necessary for the safeguarding of

- (a) the interests of the data subject; or
- (b) the rights and freedoms of any other individual

that the prohibition or restriction ought to prevail over those provisions.

(2) The Minister may by Order exempt from the non-disclosure provisions any disclosures of personal data made in circumstances specified in the Order, if he considers the exemption is necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other person.

PART VII

ENFORCEMENT

38. (1) Where the Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection principles under section 4, the Commissioner may serve him with an enforcement notice requiring him, to do either or both of the following:

- (a) take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified; or
- (b) refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing them for a purpose so specified or in a manner so specified, after such time as may be so specified.

(2) In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.

(3) An enforcement notice in respect of a contravention of the fourth data protection principle which requires the data controller to rectify, block, erase or destroy any inaccurate data may also require the data controller to rectify, block, erase or destroy any other data held by him and containing an expression of opinion which appears to the Commissioner to be based on the inaccurate data.

(4) An enforcement notice in respect of a contravention of the fourth data protection principle under section 4, in the case of data which accurately records information received or obtained by the data controller from the data subject or a third party, may require the data controller either

- (a) to rectify, block, erase or destroy any inaccurate data and any other data held by him and containing an expression of opinion which appears to the Commissioner to be based on inaccurate data; or
- (b) to take such steps as are specified in the notice for securing compliance with the requirements specified in section 9 and, if the Commissioner thinks fit, for

supplementing the data with such statement of the true facts relating to the matters dealt with by the data as the Commissioner may approve.

(5) Where

(a) an enforcement notice requires the data controller to rectify, block, erase or destroy any personal data; or

(b) the Commissioner is satisfied that personal data which has been rectified, blocked, erased or destroyed had been processed in contravention of any of the data protection principles under section 4,

an enforcement notice may, if reasonably practicable, require the data controller to notify third parties to whom the data has been disclosed of the rectification, blocking, erasure or destruction.

(6) In determining whether it is reasonably practicable to require the notification specified in subsection 5(b) regard shall be had, in particular, to the number of persons who would have to be notified.

(7) An enforcement notice must contain

(a) a statement of the data protection principle or principles under section 4, which the Commissioner is satisfied have been or are being contravened and his reasons for reaching that conclusion; and

(b) particulars of the rights of appeal conferred by section 50.

(8) Subject to subsection (9), an enforcement notice shall not require any of the provisions of the notice to be complied with before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(9) Where by reason of special circumstances the Commissioner considers that an enforcement notice should be complied with as a matter of urgency he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion.

(10) Where subsection (8) shall not apply the notice shall not require the provisions of the notice to be complied with before the end of the period of 7 days beginning with the day on which the notice is served.

39. (1) Where the Commissioner considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the data protection principles under section 4, to which it relates, he may cancel or vary the enforcement notice by written notice to the person on whom it was served.

(2) A person on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal can be brought against that enforcement notice, apply in writing to the Commissioner for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the data protection principle or principles under section 4 to which that notice relates.

40. (1) A request may be made to the Commissioner by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act.

OBJECTS AND REASONS

This Bill would provide for

- (a) the regulation of the collection, keeping, processing, use or dissemination of personal data;
- (b) the protection of the privacy of individuals in relation to personal data; and
- (c) related matters **related thereto**.

Arrangement of Sections

Section

PART I

Preliminary

1. Short title.
2. Interpretation.
3. Application of Act.

PART II

DATA PROTECTION PRINCIPLES

4. Data protection principles.
 5. The interpretation of the first data protection principle.
 6. The application of the first data protection principle.
 7. Processing of sensitive personal data.
 8. The application of the second data protection principle.
 9. The application of the fourth data protection principle.
 10. The application of the sixth data protection principle.
 11. The application of the seventh data protection principle.
 12. The application of the eighth data protection principle.
- Section*

PART III

THE DATA PROTECTION COMMISSIONER

Establishment, Functions and Powers

13. Establishment of the Commissioner.
14. Functions of the Commissioner.
15. Protection of the Commissioner.
16. Confidentiality.

PART IV

RIGHTS OF DATA SUBJECTS AND OTHERS

17. Right of access to personal data.
18. Application of section 17 where data controller is a credit reference agency.
19. Right to prevent processing likely to cause damage or distress.
20. Right to prevent processing of indirect marketing.
21. Rights in relation to automated decision making.

22. Compensation for failure to comply with certain requirements.
23. Rectification, blocking, erasure and destruction.

PART V

REGISTRATION OF DATA CONTROLLERS

24. Data Controllers must be registered.
25. Register of Data Controllers.
26. Notification of changes.

Section

PART VI

EXEMPTIONS

27. References.
28. National Security.
29. Crime and taxation.
30. Health, education and social work.
31. Regulatory activity.
32. Research, history and statistics.
33. Information available to the public by or under enactment.
34. Disclosures required by law or made in connection with legal proceedings etc.
35. Legal professional privilege.
36. Domestic purposes.
37. Powers to make further exemptions by Order.

PART VII

ENFORCEMENT

38. Enforcement notice.
39. Cancellation of enforcement notice.

40. Request for assessment.
41. Information notices.
42. Failure to comply with notice.
43. Service of notice by the Commissioner.

Section

44. Warrants.
45. Execution of warrants.
46. Matters exempt from inspection and seizure.
47. Return of warrants.
48. Obstruction of execution of a warrant.

PART VIII

DATA PROTECTION TRIBUNAL

49. Establishment of the Data Protection Appeal Tribunal.
50. Rights of appeal.
51. Determination of appeals.

PART IX

MISCELLANEOUS

52. Unlawful obtaining etc. of personal data.
53. Disclosure of information.
54. Liability of directors, etc.
55. Act binds Crown.
56. Regulations.
57. Commencement.

FIRST SCHEDULE

SECOND SCHEDULE

BARBADOS

A Bill entitled

An Act to provide for

- (a) the regulation of the collection, keeping, processing, use or dissemination of personal data;
- (b) the protection of the privacy of individuals in relation to personal data; and
- (c) related matters **related thereto**.

ENACTED by the Parliament of Barbados as follows:

PART I

Preliminary

1. This Act may be cited as the *Data Protection Act, 2005*.
2. In this Act,

"accessible public record" means any record that is kept by any authority to which members of the public are given access;

"accessible record" means

- (a) a health record;
- (b) an educational record; or
- (c) an accessible public record;

"credit reference agency" means a person carrying on a business comprising the furnishing of persons with information relevant to the financial standing of individuals, being information collected by the agency for that purpose;

"Commissioner" means Data Protection Commissioner;

"data" means information that

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

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

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or

(d) does not fall within paragraphs (a), (b) or (c) but forms part of an accessible record;

"data controller" means a person who determines the purposes for which and the manner in which any personal data is processed;

"data processor" in relation to personal data, means any person other than an employee of the data controller who processes the data on behalf of the data controller;

"data subject" means an individual who is the subject of personal data;

"personal data" means data which relates to an individual who can be identified

(a) from that data; or

(b) from other information which is in the possession of or is likely to come into the possession of the data controller;

"processing" in relation to information and data, means obtaining, recording or holding information or data or carrying out any operation or set of operations on the information and 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;

"Register" means the Register of Data Controllers required to be kept by the Data Protection Commissioner under section 25;

"relevant filing system" means any set of information or data relating

to individuals to the extent that although the information or data is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that the specific information or data relating to a particular individuals is readily accessible;

"sensitive personal data" means personal data consisting of information on a data subject's

- (a) racial or ethnic origin;
- (b) political opinions;
- (c) religious beliefs or other beliefs of a similar nature;
- [(d) membership of any organization whether [social,] economic or otherwise;]
- (e) physical or mental health or condition;
- (f) sexual orientation or sexual life;
- (g) criminal or financial record; or
- (h) proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

3. (1) Except as otherwise provided herein, this Act applies to a data controller in respect of any data if

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

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

(3) For the purposes of this section, each of the following is to be treated as established in Barbados:

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

PART II

DATA PROTECTION PRINCIPLES

4. (1) There shall be data protection principles with which a data controller shall comply in relation to all personal data processed by the data controller.

(2) The data protection principles referred to under subsection (1) are as follows:

- (a) **First Principle:** personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless there is compliance with at least one of the conditions set out in
 - (i) section 6; and
 - (ii) in the case of sensitive personal data, section 7;
- (b) **Second Principle:** personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- (c) **Third Principle:** personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- (d) **Fourth Principle:** personal data shall be accurate and, where necessary, kept up-to-date;
- (e) **Fifth Principle:** personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;

- (f) **Sixth Principle:** personal data shall be processed in accordance with the rights of data subjects under this Act;
- (g) **Seventh Principle:** appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data; and
- (h) **Eighth Principle:** personal data shall not be transferred to a country or territory outside Barbados 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.

(3) Any person who fails to comply with the data protection principles is guilty of an offence and is liable on indictment to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.

5. (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(2) Subject to subsection (3), for the purposes of the first principle, data are to be treated as having been obtained fairly if they consist of information obtained from a person who

- (a) is authorised by or under any enactment to supply it; or
- (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on Barbados.

(3) For the purposes of the first principle personal data are not to be treated as processed fairly unless

- (a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the following information:
 - (i) the identity of the data controller;
 - (ii) the identity of that representative, where a data controller has nominated a representative for the purposes of this

Act;

- (iii) the purpose or purposes for which the data are intended to be processed; and
- (iv) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair; and

(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraphs (i) to (iv) of paragraph (a);

(4) For the purposes of paragraph (b) of subsection (3), "the relevant time" means

- (a) the time when the data controller first processes the data; or
- (b) in a case where at that time disclosure to a third party within a reasonable period is envisaged,
 - (i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed;
 - (ii) if within that period the data controller becomes, or ought to become aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware; or

(iii) in any other case, the end of that period.

6. (1) The data controller shall for the purposes of the first principle process personal data only where the data subject has given his consent in writing to the processing **and the the processing is necessary**

- (a) for the performance of a contract to which the data subject is a party; or
- (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 controller is subject, other than an obligation imposed by contract;

- (d) in order to protect the vital interests of the data subject;
- (e) for the administration of justice;
- (f) for the exercise of any functions conferred on any person by or under any enactment;
- [(g) for the exercise of any functions of the **government** or a Minister of **government**;
- (h) **for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject; and**
- (i) for the exercise of any other functions of a public nature exercised in the public interest by any person.

(2) The Minister may by Order specify particular circumstances in which this subsection is or is not taken to be satisfied.

7. (1) The data controller shall not process sensitive personal data unless the data subject has given his consent in writing **and the processing**

- (a) is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
- (b) is necessary in order to protect the vital interests of the data subject or another person, in a case where
 - (i) consent cannot 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; or
- (c) is necessary 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;
- (d) is carried out in the course of its legitimate activities by any body or association which
 - (i) is not established or conducted for profit; and

- (ii) exists for political, philosophical, religious or trade-union purposes;
- (e) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
- (f) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes;
- (g) does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (h) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
- (i) the purpose of obtaining legal advice;
- (j) the purposes of establishing, exercising or defending legal rights;
- (k) the administration of justice;
- (l) the exercise of any functions conferred on any person by or under an enactment;
- (m) the exercise of any functions of the Crown, a Minister of the Crown or a government department;
- (n) is necessary for medical purposes and is undertaken by
 - (i) a health professional;
 - (ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional;
 - (iii) in this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services;
- (o) is of sensitive personal data consisting of information as to racial or ethnic origin;
- (p) is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between

persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
(q) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

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

8. (1) For the purposes of the application of the second data protection principle the purpose for which personal data are obtained shall be specified

(a) in a notice given by the data controller to the data subject; or

(b) in a notification given to the Commissioner under Part IV of this Act.

(2) In determining whether any disclosure of personal data is compatible with the purpose for which the data were obtained, regard is to be had to the purpose for which the personal data are intended to be processed by any person to whom they are disclosed.

9. The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where

(a) having regard to the purpose for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and

(b) if the data subject has notified the data controller of the data subject's view that the data is inaccurate and the data indicates that fact.

10. A person is to be regarded as contravening the sixth principle if, but only if he contravenes

(a) section 17 by failing to supply information in accordance with that section;

(b) section 19 by failing to comply with a notice given under subsection (1) of that section to the extent that the

- notice is justified or by failing to give a notice under subsection (3) of that section;
- (c) section 20 by failing to comply with a notice given under subsection (1) of that section; or
 - (d) section 21 by failing to comply with a notice given under subsection (1) or (2) of that section or by failing to give a notification under subsection (3) of that section or a notice under subsection (4) of that section.

11. For the purposes of the application of the seventh data protection principle and having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to

- (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle; and
- (b) the nature of the data to be protected.

(2) The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

(3) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle

- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- (b) take reasonable steps to ensure compliance with those measures.

(4) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless

- (a) the processing is carried out under a contract
 - (i) which is made or evidenced in writing; and
 - (ii) under which the data processor is to act only on

instructions from the data controller; and

- (b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

12. (1) For the purposes of the application of the eighth data protection principle, an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to

- (a) the nature of the personal data;
- (b) the country or territory of origin of the information contained in the data;
- (c) the country or territory of final destination of that information;
- (d) the purposes for which and period during which the data are intended to be processed;
- (e) the law in force in the country or territory in question;
- (f) the international obligations of that country or territory;
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory whether generally or by arrangement in particular cases; and
- (h) any security measures taken in respect of the data in that country or territory.

(2) The eighth data protection principle shall not apply where

- (a) the data subject has given his consent to the transfer;
- (b) the transfer is necessary for
 - (i) the performance of a contract between the data subject and the data controller;
 - (ii) the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller;
 - (iii) the conclusion of a contract between the data controller and a person other than the data subject

which

- (A) is entered into at the request of the data subject; or
 - (B) is in the interests of the data subject;
 - (iv) the performance of a contract under paragraph (b)(iii);
 - (v) reasons of substantial public interest;
 - (vi) the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (vii) the purpose of obtaining legal advice;
 - (viii) the purposes of establishing, exercising or defending legal rights; or
 - (ix) the protection of the vital interests of the data subject;
- (c) the transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer;
- (d) the transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; or
- (e) the transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.
- (3) The Minister may by Order specify
- (a) circumstances in which a transfer is to be taken for the purposes of **subsection (1)** to be necessary for reasons of substantial public interest; and
 - (b) circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purpose of **subsection (1)** to be necessary for reasons of substantial public interest.

PART III

THE DATA PROTECTION COMMISSIONER

Establishment, Functions and Powers

13. (1) There shall be a Commissioner called the Data Protection Commissioner, who shall be appointed in the manner set out in the *First Schedule*.

(2) The *First Schedule* has effect with respect to the Commissioner and otherwise in relation thereto.

14. The functions of the Commissioner are to

- (a) promote, by education and publicity, an understanding and acceptance of the data protection principles and of the objects of those principles;
- (b) when requested to do so by a person or agency, conduct an audit of personal data maintained by that person or agency for the purpose of ascertaining whether or not the information is maintained according to the data protection principles;
- (c) monitor the use of personal data and sensitive personal data, and to report to the Minister from time to time on the results of that monitoring, including any recommendations relating to the need for, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the privacy of a person;
- (d) examine any proposed legislation that makes provisions for
 - (i) the collection of personal data by any public sector agency; or
 - (ii) the disclosure of personal data by one public sector agency to any other public sector agencyand report to the responsible Minister the results of that examination;
- (e) receive and invite representations from members of the public on any matter affecting the privacy of a person;
- (f) consult and co-operate with other persons and bodies concerned with the privacy of a person;
- (g) make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that

- person in the interests of the privacy of a person;
- (h) provide advice, with or without a request, to a Minister or an agency on any matter relevant to the operation of this Act;
 - (i) inquire generally into any matter, including any enactment, 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 a person is being or may be infringed thereby;
 - (j) undertake research into, and to monitor developments in data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons are minimised, and to report to the Minister the results of such research and monitoring;
 - (k) examine any proposed legislation or proposed policy of the Government that the Commissioner considers may affect the privacy of persons, and to report to the Minister the results of that examination;
 - (l) report, with or without request, to the Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of a person;
 - (m) report to the Minister from time to time on the desirability of the acceptance, by Barbados, of any international instrument relating to the privacy of the person and advise on the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of a person;
 - (n) prepare appropriate codes of practice for the guidance of business persons and institutions handling personal data;
 - (o) investigate complaints from persons concerning abuses in the use of personal data;
 - (p) do anything incidental or conducive to the performance of any of the preceding functions; and
 - (q) exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

15. No action or other proceeding for damages shall be instituted against a Commissioner for an act done in good faith in the

performance of a duty or in the exercise of a power under this Act.

16. (1) No person who is or who has been the Commissioner, a member of the Commissioner's staff or an agent of the Commissioner shall make use, either directly or indirectly, of any information obtained as a result of his performance of his duties or otherwise for his own benefit or advantage.

(2) No person who is or who has been the Commissioner, a member of the Commissioner's staff or an agent of the Commissioner shall disclose any information which

- (a) has been obtained by or furnished to the Commissioner under or for the purposes of this Act;
- (b) relates to an identified or identifiable person or business; and
- (c) is not at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.

(3) For the purposes of subsection (2) a disclosure of information is made with lawful authority only if and to the extent that

- (a) the disclosure is made with the consent of the individual or of the person for the time being carrying on the business;
- (b) the information was provided for the purpose of its being made available to the public under any provision of this Act;
- (c) the disclosure is made for the purposes of and is necessary for, the discharge of any function under this Act;
- (d) the disclosure is made for the purposes of any proceedings, whether criminal or civil and whether arising under or by virtue of this Act or otherwise; or
- (e) having regard to the rights and freedoms or legitimate interests of any person, the disclosure is necessary in the public interest.

(4) Any person who contravenes subsections (1) or (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 and to imprisonment for 6 months.

PART IV

RIGHTS OF DATA SUBJECTS AND OTHERS

17. (1) Subject to the provisions of this Act, a person has the right
- (a) to be informed by the data controller whether the personal data of which that person is the data subject is being processed by or on behalf of the data controller;
 - (b) where personal data of the data subject is being processed by or on behalf of the data controller, to request the data controller to supply the data subject with a description of
 - (i) the personal data of which that person is the data subject;
 - (ii) the purposes for which the personal data is processed;
 - (iii) the recipients or classes of recipients to whom they are or may be disclosed; and
 - (iv) where processing by automatic means of sensitive personal data of the data subject for the purpose of evaluating matters related to him and is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in the decision taking.
 - (c) to have communicated to the data subject in an intelligible form
 - (i) information constituting any personal data of the data subject; and
 - (ii) any information available to the data controller as to the source of that data.
- (2) A data controller is not obliged to supply any information under subsection (1) unless the data controller has received
- (a) a request in writing; and
 - (b) such fee as the Minister may prescribe.
- (3) A data controller is not obliged to comply with a request under this section unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the data subject making the request and to locate the information that the data subject seeks.

(4) Where a data controller cannot comply with the request under this section without disclosing information relating to a third party who can be identified from that information, the data controller is not obliged to comply with the request unless

- (a) the third party has consented to the disclosure of the information to the data subject making the request; and
- (b) it is reasonable in all the circumstances to comply with the request without the consent of the third party.

(5) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the third party concerned, regard shall be had, in particular to

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

(6) Where a data controller refuses to comply with a request under this section he shall give reasons in writing for his refusal.

(7) A person aggrieved by the decision of the data controller may appeal to the Commissioner.

(8) Subject to subsection (4), a data controller shall comply with a request under this section within 30 days of the date of receipt of that request.

18. (1) Where the data controller is a credit reference agency, section 9 has effect subject to the provisions of this section.

(2) A person making a request under section 17 may limit his request to personal data relevant to his financial standing, and shall be taken to have so limited his request unless the request shows a contrary intention.

(3) Where the data controller receives a request under section 17 in a case where personal data of which the person making the request is the data subject is being processed by or on behalf of the data controller, the obligation to supply information under that section includes an obligation to give the person making the request a

statement, in such a form as may be prescribed by the Minister, of the person's rights.

19. (1) Subject to subsection (2), a data subject is entitled to require the data controller at the end of a 21 day period by notice in writing, to cease, or not begin processing or processing for a specified purpose or in a specified manner, any personal data in respect of which he is the data subject, on the grounds that,

- (a) the processing of that data or the data controller's processing for that purpose or in that manner is causing or is likely to cause substantial damage or distress to the data subject or another; and
- (b) damage or distress is or would be unwarranted.

(2) Subsection (1) does not apply

- (a) in a case where any of the conditions in paragraphs 1(a) to (b)(iv) of section 6(1); or
- (b) in such other cases as may be prescribed by the Minister by Order.

(3) The data controller shall within 21 days of receiving a notice under subsection (1) give the data subject written notice

- (a) stating that he has complied or intends to comply with the data subject's notice;
- (b) stating reasons for his refusal to comply with a data subject's notice; or
- (c) stating the reasons for complying with part of the data subject's notice and the extent of that compliance.

(4) If a court is satisfied, on the application of any data subject who has given notice under subsection (1), that the data controller in question has failed to comply with the notice, the court may order the data controller to take such steps for complying with that notice as the court sees fit.

20. (1) A data subject is entitled at any time by notice in writing to a data controller to require the data controller at the end of a 21 day period to cease, processing for the purposes of direct marketing personal data in respect of which he is the data subject.

(2) If a court is satisfied, on the application of data subject who has given notice under subsection (1), that the data controller has failed to comply with the notice, the court may order data controller to take such steps for complying with the notice as the court sees fit.

(3) For the purposes of this section "indirect marketing" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

21. (1) An **individual** is entitled at any time, by notice in writing to a data controller, to require the data controller to ensure that no decision is taken by or on behalf of the data which significantly affects that **individual** and is based solely on processing by automatic means of sensitive personal data for the purpose of evaluating matters related to the **individual**

(2) A data controller shall inform a data subject by notice of any decision made by the data controller or on the half of the data controller which is made solely on the processing by automatic means of sensitive personal data for the purpose of evaluating any matters related to that data subject.

(3) The data subject is entitled, within 21 days of receiving that notification from the data controller under subsection (2), by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.

(4) The data controller shall within 21 days of receiving a notice under subsection (3) give the individual a written notice specifying the steps that the data controller intends to take to comply with the data subject's notice.

(5) A notice under subsection (1) does not have effect in relation to an exempt decision; and nothing in subsection (2) applies to an exempt decision.

(6) For the purposes of this section "exempt decision" means any decision

- (a) in respect of which the conditions in subsections (7) and (8) are met; or
- (b) which is made in such other circumstances as may be prescribed by the Minister.

(7) The condition in this subsection is that the decision

- (a) is taken in the course of steps taken
 - (i) for the purpose of considering whether to enter into a contract with the data subject;

- (ii) with a view to entering into such contract;
- (iii) in the course of performing such a contract; or
- (b) is authorised or required by or under any enactment.
- (8) The condition in this subsection is that either
 - (a) the effect of the decision is to grant a request of the data subject; or
 - (b) steps have now been taken to safeguard the legitimate interests of the data subject.

(9) If a court is satisfied, on the application of the data subject that a data controller taking a decision in respect of that data subject has failed to comply with subsection (1) or subsection (2), the court may order the data controller to reconsider the decision, or to take a new decision which is not based solely on processing by automatic means.

22. (1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress where

- (a) the individual also suffers damage by reason of the contravention; or
- (b) the contravention relates to the processing of personal data for
 - (i) the purposes of journalism;
 - (ii) artistic purposes; or
 - (iii) literary purposes.

(3) In proceedings brought against a person by virtue of this section it is a defence to prove that the data controller had taken such care as all the circumstances reasonably required to comply with the requirements concerned.

23. (1) Where a court is satisfied on the application of a data subject that personal data of which the applicant is the subject is inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contains an expression of opinion which appears to the court to be based on the inaccurate data.

(2) Subsection (1) applies whether or not the data accurately records information received or obtained by the data controller from the data subject or a third party but where the data accurately records such information, where

- (a) the requirements mentioned in section 9 have been complied with, the court may, instead of making an order under subsection (1), make an order requiring the data to be supplemented by such statement of the true facts relating to the matters dealt with by the data as the court may approve; and
- (b) all or any of those requirements have not been complied with, the court may, instead of making an order under that subsection, make such order as it thinks fit for securing compliance with those requirements with or without a further order requiring the data to be supplemented by such a statement as is mentioned in paragraph (a).

(3) Where the court

- (a) makes an order under subsection (1); or
- (b) is satisfied on the application of a data subject that personal data of which he was the data subject and which have been rectified, blocked, erased or destroyed were inaccurate,

it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.

(4) Where a court is satisfied on the application of a data subject

- (a) that he has suffered damage by reason of any contravention by a data controller of any of the requirements of this Act in respect of any personal data, in circumstances entitling him to compensation under section 22; and
- (b) that there is a substantial risk of further contravention in

respect of those data in such circumstances,
the court may order the rectification, blocking, erasure or destruction of any of those data.

(5) Where the court makes an order under subsection (4) it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.

(6) In determining whether it is reasonably practicable to require such notification as is mentioned in subsection (3) or (5) the court shall have regard, in particular, to the number of persons who would have to be notified.

PART V

REGISTRATION OF DATA CONTROLLERS

24. (1) A person shall not operate as a data controller unless he is registered in the Register of Data Controllers, maintained by the Commissioner and referred to in section 25.

(2) A person who desires to operate as a data controller may

(a) on making an application to the Commissioner in the form prescribed by the Minister; and

(b) on payment to the Commissioner of the prescribed fee

obtain a certificate from the Commissioner for that purpose.

(3) A person who operates without being registered in the manner described under this section shall be liable on summary conviction to pay a fine of \$5 000 or to a term of imprisonment of 2 months or to both.

25. (1) The Commissioner shall keep a register to be known as the Register of Data Controllers in which he shall cause to be entered in relation to the data controller, the following particulars:

(a) the name and address;

(b) the date of registration;

(c) a description of the personal data processed by or on behalf of the data controller and of the category or categories of data subject to which they relate;

- (d) a description of the purpose or purposes for which the data is processed;
- (e) a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data; and
- (f) the names, or a description of, any countries or territories outside the Caribbean Community to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data.

(2) The Register shall at all reasonable times be open to inspection at the Office **of the Commissioner**.

(3) The Commissioner shall make all amendments to the Register as are necessary.

26. (1) The data controller has a duty to notify the Commissioner of any changes which may affect the particulars entered by the Commissioner in the Register.

(2) A data controller who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$1 000 or to imprisonment for a term of **3 months** and the Commissioner may remove that data controller from the Register.

(3) On receiving notification of the data controller under subsection (1) the Commissioner shall make such amendments to the Register as are necessary.

PART VI

EXEMPTIONS

27. (1) In this Part "the subject information provisions" means

- (a) the first data protection principle to the extent to which it requires compliance with section 5(2); and
- (b) section 17.

(2) In this part "the non-disclosure provisions" means

- (a) the first data protection principle, except to the extent to which it requires compliance with section 6 and section 7;
- (b) the second, third, fourth and fifth data protection principles under section 4; and

(c) sections 19 and 23(1) to (3)

to the extent to which they are inconsistent with the disclosure in question.

(3) Except as provided by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorizing the withholding of information.

28. (1) Personal data is exempt from

(a) section 5;

(b) Parts IV and V; and

(c) section 52

where the exemption from **those provisions** is required for the purpose of safeguarding national security.

29. (1) Personal data processed for

(a) the prevention or detection of crime;

(b) the apprehension or prosecution of offenders; or

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

is exempt from the first data protection principle, except to the extent to which it requires compliance with the conditions in section 6, section 7 and section 17 in any case to the extent to which the application of those provisions to the data is likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data which

(a) is processed for the purpose of discharging statutory functions; and

(b) consists of information obtained for such a purpose from a person who had it in his possession for any of the purposes under subsection (1)

is exempt from the subject information provisions to the same extent as personal data processed for any of the purposes under subsection (1).

(3) Personal data is exempt from the non-disclosure provisions in any case in which

- (a) the disclosure is for any of the purpose under subsection (1); and
- (b) the application of those provisions in relation to disclosure is likely to prejudice any of the matters mentioned under subsection (1).

(4) Personal data in respect of which the data controller is a government department, which

- (a) consist of a classification applied to the data subject as a part of a system of risk assessment which is operated by the relevant authority for
 - (i) the assessment or collection of any tax, duty or of any imposition of a similar nature; or
 - (ii) the prevention or detection of crime, or apprehension or prosecution of offenders, where the offence involves any unlawful claim for payment out of or any unlawful application of public funds; and
- (b) is processed for either of those purposes

is exempt from section 17 to the extent to which the exemption is required in the interests of the operation of the system.

30. (1) The Minister may by Order exempt from the subject information provisions, or modify those provisions in relation to personal data

- (a) consisting of information as to the physical or mental health or condition of a data subject;
- (b) in respect of which the data controller is an educational institution within the meaning assigned to it under section 2 of the *Education Act*, and which consists of information relating to persons who are or have been pupils at the educational institution;
- (c) in respect of which the data controller is a tertiary institution within the meaning assigned to it under section 2 of the *Education Act*, and which consists of information relating to persons who are or have been students at the tertiary institution;

- (d) of other descriptions as may be specified in the Order, being information processed
 - (i) by government departments, public service, charities or other entities designated by or under the Order; and
 - (ii) in the course of, or for the purposes of carrying out social work in relation to the data subject

to the extent that the Minister is satisfied that the carrying out of social work is likely to be prejudiced.

31. (1) Personal data processed for the purposes of discharging functions to which this subsection applies is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is designed for the purpose of

- (a) protecting members of the public against
 - (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or 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 authorised to carry on any profession or other activity;
- (b) protecting charities against misconduct or mismanagement, whether by trustees or other persons in their administration;
- (c) protecting the property of charities from loss or misapplication;
- (d) the recovery of the property of charities;
- (e) securing the health, safety and welfare of persons at work; or

(f) 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.

(3) In subsection (2) "relevant function" means

(a) any function conferred on any person by or under any enactment;

(b) any function of a Minister or government department; or

(c) any other function which is of a public nature and is exercised in the public interest.

(4) Personal data processed for the purpose of discharging any function which is designed for protecting members of the public against

(a) maladministration by public bodies;

(b) failure in services provided by public bodies; or

(c) a failure of a public body to provide a service which is a function of the body to provide

is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data is likely to prejudice the proper discharge of that function.

(5) Personal data processed for the purpose of discharging any function which is designed for

(a) protecting members of the public against conduct which may adversely affect their interests by persons carrying on a business;

(b) 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

(c) regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market

is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

32. (1) In this section

"research purposes" includes statistical or historical purposes;

"the relevant conditions", in relation to any processing of personal data, means the conditions

- (a) that the data are not processed to support measures or decisions with respect to particular individuals; and
- (b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be caused to any data subject.

(2) For the purposes of the second data protection principle under section 5, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(3) Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle under section 5, be kept indefinitely.

(4) Personal data which are processed only for research purposes is exempt from section 17 if

- (a) they are processed in compliance with the relevant conditions; and
- (b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

(5) For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed

- (a) to any person, for research purposes only;
- (b) to the data subject or a person acting on his behalf;
- (c) at the request, or with the consent, of the data subject or a person acting on his behalf; or
- (d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c).

33. Personal data are exempt from

- (a) the subject information provisions;
- (b) the fourth data protection principle under section 5 and section 22(1) to (3); and
- (c) the non-disclosure provisions

if the data consist of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

34. (1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

- (2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary
 - (a) for the purpose of, or in connection with, any legal proceedings including prospective legal proceedings; or
 - (b) for the purpose of obtaining legal advice

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

35. Personal data is exempt from the subject information provisions if the data consists of information in respect of which a claim to legal professional privilege applies.

36. Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs including recreational purposes is exempt from the data protection principles under section 5 and the provisions of Parts IV and V.

37. (1) The Minister may by Order exempt from the subject information provisions personal data consisting of information the disclosure of which is prohibited or restricted by or under any enactment if and to the extent that he considers it necessary for the safeguarding of

- (a) the interests of the data subject; or
- (b) the rights and freedoms of any other individual

that the prohibition or restriction ought to prevail over those provisions.

(2) The Minister may by Order exempt from the non-disclosure provisions any disclosures of personal data made in circumstances specified in the Order, if he considers the exemption is necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other person.

OBJECTS AND REASONS

This Bill would provide for

- (a) the regulation of the collection, keeping, processing, use or dissemination of personal data;
- (b) the protection of the privacy of individuals in relation to personal data; and
- (c) related matters **related thereto**.

Arrangement of Sections

Section

PART I

Preliminary

1. Short title.
2. Interpretation.
3. Application of Act.

PART II

DATA PROTECTION PRINCIPLES

4. Data protection principles.
5. The interpretation of the first data protection principle.
6. The application of the first data protection principle.
7. Processing of sensitive personal data.
8. The application of the second data protection principle.
9. The application of the fourth data protection principle.

10. The application of the sixth data protection principle.
11. The application of the seventh data protection principle.
12. The application of the eighth data protection principle.

Section

PART III

THE DATA PROTECTION COMMISSIONER

Establishment, Functions and Powers

13. Establishment of the Commissioner.
14. Functions of the Commissioner.
15. Protection of the Commissioner.
16. Confidentiality.

PART IV

RIGHTS OF DATA SUBJECTS AND OTHERS

17. Right of access to personal data.
18. Application of section 17 where data controller is a credit reference agency.
19. Right to prevent processing likely to cause damage or distress.
20. Right to prevent processing of indirect marketing.
21. Rights in relation to automated decision making.
22. Compensation for failure to comply with certain requirements.
23. Rectification, blocking, erasure and destruction.

PART V

REGISTRATION OF DATA CONTROLLERS

24. Data Controllers must be registered.
25. Register of Data Controllers.
26. Notification of changes.

Section

PART VI
EXEMPTIONS

27. References.
28. National Security.
29. Crime and taxation.
30. Health, education and social work.
31. Regulatory activity.
32. Research, history and statistics.
33. Information available to the public by or under enactment.
34. Disclosures required by law or made in connection with legal proceedings etc.
35. Legal professional privilege.
36. Domestic purposes.
37. Powers to make further exemptions by Order.

PART VII
ENFORCEMENT

38. Enforcement notice.
39. Cancellation of enforcement notice.
40. Request for assessment.
41. Information notices.
42. Failure to comply with notice.
43. Service of notice by the Commissioner.

Section

44. Warrants.
45. Execution of warrants.
46. Matters exempt from inspection and seizure.

47. Return of warrants.

48. Obstruction of execution of a warrant.

PART VIII

DATA PROTECTION TRIBUNAL

49. Establishment of the Data Protection Appeal Tribunal.

50. Rights of appeal.

51. Determination of appeals.

PART IX

MISCELLANEOUS

52. Unlawful obtaining etc. of personal data.

53. Disclosure of information.

54. Liability of directors, etc.

55. Act binds Crown.

56. Regulations.

57. Commencement.

FIRST SCHEDULE

SECOND SCHEDULE

A Bill entitled

An Act to provide for

- (a) the regulation of the collection, keeping, processing, use or dissemination of personal data;
- (b) the protection of the privacy of individuals in relation to personal data; and
- (c) related matters **related thereto**.

ENACTED by the Parliament of Barbados as follows:

PART I

Preliminary

1. This Act may be cited as the *Data Protection Act, 2005*.
2. In this Act,

"accessible public record" means any record that is kept by any authority to which members of the public are given access;

"accessible record" means

- (a) a health record;
- (b) an educational record; or
- (c) an accessible public record;

"credit reference agency" means a person carrying on a business comprising the furnishing of persons with information relevant to the financial standing of individuals, being information collected by the agency for that purpose;

"Commissioner" means Data Protection Commissioner;

"data" means information that

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

- (b) is recorded with the intention that it should be processed by means of such equipment;
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or
- (d) does not fall within paragraphs (a), (b) or (c) but forms part of an accessible record;

"data controller" means a person who determines the purposes for which and the manner in which any personal data is processed;

"data processor" in relation to personal data, means any person other than an employee of the data controller who processes the data on behalf of the data controller;

"data subject" means an individual who is the subject of personal data;

"personal data" means data which relates to an individual who can be identified

- (a) from that data; or
- (b) from other information which is in the possession of or is likely to come into the possession of the data controller;

"processing" in relation to information and data, means obtaining, recording or holding information or data or carrying out any operation or set of operations on the information and 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;

"Register" means the Register of Data Controllers required to be kept by the Data Protection Commissioner under section 25;

"relevant filing system" means any set of information or data relating to individuals to the extent that although the information or data is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is

structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that the specific information or data relating to a particular individuals is readily accessible;

"sensitive personal data" means personal data consisting of information on a data subject's

- (a) racial or ethnic origin;
- (b) political opinions;
- (c) religious beliefs or other beliefs of a similar nature;
- [(d) membership of any organization whether [social,] economic or otherwise;]
- (e) physical or mental health or condition;
- (f) sexual orientation or sexual life;
- (g) criminal or financial record; or
- (h) proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

3. (1) Except as otherwise provided herein, this Act applies to a data controller in respect of any data if

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

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

(3) For the purposes of this section, each of the following is to be treated as established in Barbados:

- (a) an individual who is ordinarily resident in Barbados or the Caribbean Community;

- (b) a body incorporated under the *Companies Act*;
- (c) a partnership or other unincorporated association formed under the laws of Barbados; and
- (d) any person who does not fall within paragraphs (a), (b) and (c) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing.

PART II

DATA PROTECTION PRINCIPLES

4. (1) There shall be data protection principles with which a data controller shall comply in relation to all personal data processed by the data controller.

(2) The data protection principles referred to under subsection (1) are as follows:

- (a) **First Principle:** personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless there is compliance with at least one of the conditions set out in
 - (i) section 6; and
 - (ii) in the case of sensitive personal data, section 7;
- (b) **Second Principle:** personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
- (c) **Third Principle:** personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- (d) **Fourth Principle:** personal data shall be accurate and, where necessary, kept up-to-date;
- (e) **Fifth Principle:** personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;
- (f) **Sixth Principle:** personal data shall be processed in accordance with the rights of data subjects under this Act;

(g) **Seventh Principle:** appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to personal data; and

(h) **Eighth Principle:** personal data shall not be transferred to a country or territory outside Barbados 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.

(3) Any person who fails to comply with the data protection principles is guilty of an offence and is liable on indictment to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.

5. (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.

(2) Subject to subsection (3), for the purposes of the first principle, data are to be treated as having been obtained fairly if they consist of information obtained from a person who

(a) is authorised by or under any enactment to supply it; or

(b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on Barbados.

(3) For the purposes of the first principle personal data are not to be treated as processed fairly unless

(a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the following information:

(i) the identity of the data controller;

(ii) the identity of that representative, where a data controller has nominated a representative for the purposes of this Act;

(iii) the purpose or purposes for which the data are intended

to be processed; and

- (iv) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair; and
 - (b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraphs (i) to (iv) of paragraph (a);
- (4) For the purposes of paragraph (b) of subsection (3), "the relevant time" means
- (a) the time when the data controller first processes the data; or
 - (b) in a case where at that time disclosure to a third party within a reasonable period is envisaged,
 - (i) if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed;
 - (ii) if within that period the data controller becomes, or ought to become aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware; or
 - (iii) in any other case, the end of that period.

6. (1) The data controller shall for the purposes of the first principle process personal data only where the data subject has given his consent in writing to the processing **and the the processing is necessary**

- (a) for the performance of a contract to which the data subject is a party; or
- (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 controller is subject, other than an obligation imposed by contract;
- (d) in order to protect the vital interests of the data subject;

- (e) for the administration of justice;
- (f) for the exercise of any functions conferred on any person by or under any enactment;
- [(g) for the exercise of any functions of the **government** or a Minister of **government**;
- (h) **for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject; and**
- (i) for the exercise of any other functions of a public nature exercised in the public interest by any person.

(2) The Minister may by Order specify particular circumstances in which this subsection is or is not taken to be satisfied.

7. (1) The data controller shall not process sensitive personal data unless the data subject has given his consent in writing **and the processing**

- (a) is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment;
- (b) is necessary in order to protect the vital interests of the data subject or another person, in a case where
 - (i) consent cannot 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; or
- (c) is necessary 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;
- (d) is carried out in the course of its legitimate activities by any body or association which
 - (i) is not established or conducted for profit; and
 - (ii) exists for political, philosophical, religious or trade-union purposes;

- (e)* is carried out with appropriate safeguards for the rights and freedoms of data subjects;
- (f)* relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes;
- (g)* does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (h)* is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
- (i)* the purpose of obtaining legal advice;
- (j)* the purposes of establishing, exercising or defending legal rights;
- (k)* the administration of justice;
- (l)* the exercise of any functions conferred on any person by or under an enactment;
- (m)* the exercise of any functions of the Crown, a Minister of the Crown or a government department;
- (n)* is necessary for medical purposes and is undertaken by
 - (i)* a health professional;
 - (ii)* a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional;
 - (iii)* in this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services;
- (o)* is of sensitive personal data consisting of information as to racial or ethnic origin;
- (p)* is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and

(q) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

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

8. (1) For the purposes of the application of the second data protection principle the purpose for which personal data are obtained shall be specified

(a) in a notice given by the data controller to the data subject; or

(b) in a notification given to the Commissioner under Part IV of this Act.

(2) In determining whether any disclosure of personal data is compatible with the purpose for which the data were obtained, regard is to be had to the purpose for which the personal data are intended to be processed by any person to whom they are disclosed.

9. The fourth principle is not to be regarded as being contravened by reason of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where

(a) having regard to the purpose for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and

(b) if the data subject has notified the data controller of the data subject's view that the data is inaccurate and the data indicates that fact.

10. A person is to be regarded as contravening the sixth principle if, but only if he contravenes

(a) section 17 by failing to supply information in accordance with that section;

(b) section 19 by failing to comply with a notice given under subsection (1) of that section to the extent that the notice is justified or by failing to give a notice under subsection (3) of that section;

- (c) section 20 by failing to comply with a notice given under subsection (1) of that section; or
- (d) section 21 by failing to comply with a notice given under subsection (1) or (2) of that section or by failing to give a notification under subsection (3) of that section or a notice under subsection (4) of that section.

11. For the purposes of the application of the seventh data protection principle and having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to

- (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle; and
- (b) the nature of the data to be protected.

(2) The data controller must take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

(3) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle

- (a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out; and
- (b) take reasonable steps to ensure compliance with those measures.

(4) Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless

- (a) the processing is carried out under a contract
 - (i) which is made or evidenced in writing; and
 - (ii) under which the data processor is to act only on instructions from the data controller; and
- (b) the contract requires the data processor to comply with

obligations equivalent to those imposed on a data controller by the seventh principle.

12. (1) For the purposes of the application of the eighth data protection principle, an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to

- (a) the nature of the personal data;
- (b) the country or territory of origin of the information contained in the data;
- (c) the country or territory of final destination of that information;
- (d) the purposes for which and period during which the data are intended to be processed;
- (e) the law in force in the country or territory in question;
- (f) the international obligations of that country or territory;
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory whether generally or by arrangement in particular cases; and
- (h) any security measures taken in respect of the data in that country or territory.

(2) The eighth data protection principle shall not apply where

- (a) the data subject has given his consent to the transfer;
- (b) the transfer is necessary for
 - (i) the performance of a contract between the data subject and the data controller;
 - (ii) the taking of steps at the request of the data subject with a view to his entering into a contract with the data controller;
 - (iii) the conclusion of a contract between the data controller and a person other than the data subject which
 - (A) is entered into at the request of the data

subject; or

(B) is in the interests of the data subject;

- (iv) the performance of a contract under paragraph (b)(iii);
 - (v) reasons of substantial public interest;
 - (vi) the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings);
 - (vii) the purpose of obtaining legal advice;
 - (viii) the purposes of establishing, exercising or defending legal rights; or
 - (ix) the protection of the vital interests of the data subject;
- (c) the transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer;
- (d) the transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; or
- (e) the transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.
- (3) The Minister may by Order specify
- (a) circumstances in which a transfer is to be taken for the purposes of **subsection (1)** to be necessary for reasons of substantial public interest; and
 - (b) circumstances in which a transfer which is not required by or under an enactment is not to be taken for the purpose of **subsection (1)** to be necessary for reasons of substantial public interest.

PART III

THE DATA PROTECTION COMMISSIONER

Establishment, Functions and Powers

13. (1) There shall be a Commissioner called the Data Protection Commissioner, who shall be appointed in the manner set out in the *First Schedule*.

(2) The *First Schedule* has effect with respect to the Commissioner and otherwise in relation thereto.

14. The functions of the Commissioner are to

- (a) promote, by education and publicity, an understanding and acceptance of the data protection principles and of the objects of those principles;
- (b) when requested to do so by a person or agency, conduct an audit of personal data maintained by that person or agency for the purpose of ascertaining whether or not the information is maintained according to the data protection principles;
- (c) monitor the use of personal data and sensitive personal data, and to report to the Minister from time to time on the results of that monitoring, including any recommendations relating to the need for, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the privacy of a person;
- (d) examine any proposed legislation that makes provisions for
 - (i) the collection of personal data by any public sector agency; or
 - (ii) the disclosure of personal data by one public sector agency to any other public sector agencyand report to the responsible Minister the results of that examination;
- (e) receive and invite representations from members of the public on any matter affecting the privacy of a person;
- (f) consult and co-operate with other persons and bodies concerned with the privacy of a person;
- (g) make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interests of the privacy of a person;
- (h) provide advice, with or without a request, to a Minister or an

- agency on any matter relevant to the operation of this Act;
- (i) inquire generally into any matter, including any enactment, 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 a person is being or may be infringed thereby;
 - (j) undertake research into, and to monitor developments in data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons are minimised, and to report to the Minister the results of such research and monitoring;
 - (k) examine any proposed legislation or proposed policy of the Government that the Commissioner considers may affect the privacy of persons, and to report to the Minister the results of that examination;
 - (l) report, with or without request, to the Minister from time to time on any matter affecting the privacy of the individual, including the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of a person;
 - (m) report to the Minister from time to time on the desirability of the acceptance, by Barbados, of any international instrument relating to the privacy of the person and advise on the need for, or desirability of, taking legislative, administrative, or other action to give protection or better protection to the privacy of a person;
 - (n) prepare appropriate codes of practice for the guidance of business persons and institutions handling personal data;
 - (o) investigate complaints from persons concerning abuses in the use of personal data;
 - (p) do anything incidental or conducive to the performance of any of the preceding functions; and
 - (q) exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

15. No action or other proceeding for damages shall be instituted against a Commissioner for an act done in good faith in the performance of a duty or in the exercise of a power under this Act.

16. (1) No person who is or who has been the Commissioner, a

member of the Commissioner's staff or an agent of the Commissioner shall make use, either directly or indirectly, of any information obtained as a result of his performance of his duties or otherwise for his own benefit or advantage.

(2) No person who is or who has been the Commissioner, a member of the Commissioner's staff or an agent of the Commissioner shall disclose any information which

- (a) has been obtained by or furnished to the Commissioner under or for the purposes of this Act;
- (b) relates to an identified or identifiable person or business; and
- (c) is not at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority.

(3) For the purposes of subsection (2) a disclosure of information is made with lawful authority only if and to the extent that

- (a) the disclosure is made with the consent of the individual or of the person for the time being carrying on the business;
- (b) the information was provided for the purpose of its being made available to the public under any provision of this Act;
- (c) the disclosure is made for the purposes of and is necessary for, the discharge of any function under this Act;
- (d) the disclosure is made for the purposes of any proceedings, whether criminal or civil and whether arising under or by virtue of this Act or otherwise; or
- (e) having regard to the rights and freedoms or legitimate interests of any person, the disclosure is necessary in the public interest.

(4) Any person who contravenes subsections (1) or (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 and to imprisonment for 6 months.

PART IV

RIGHTS OF DATA SUBJECTS AND OTHERS

17. (1) Subject to the provisions of this Act, a person has the right

- (a) to be informed by the data controller whether the personal data of which that person is the data subject is being processed by or on behalf of the data controller;
 - (b) where personal data of the data subject is being processed by or on behalf of the data controller, to request the data controller to supply the data subject with a description of
 - (i) the personal data of which that person is the data subject;
 - (ii) the purposes for which the personal data is processed;
 - (iii) the recipients or classes of recipients to whom they are or may be disclosed; and
 - (iv) where processing by automatic means of sensitive personal data of the data subject for the purpose of evaluating matters related to him and is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in the decision taking.
 - (c) to have communicated to the data subject in an intelligible form
 - (i) information constituting any personal data of the data subject; and
 - (ii) any information available to the data controller as to the source of that data.
- (2) A data controller is not obliged to supply any information under subsection (1) unless the data controller has received
- (a) a request in writing; and
 - (b) such fee as the Minister may prescribe.
- (3) A data controller is not obliged to comply with a request under this section unless he is supplied with such information as he may reasonably require in order to satisfy himself as to the identity of the data subject making the request and to locate the information that the data subject seeks.
- (4) Where a data controller cannot comply with the request under this section without disclosing information relating to a third party who can be identified from that information, the data controller is not obliged to comply with the request unless
- (a) the third party has consented to the disclosure of the

information to the data subject making the request; and

(b) it is reasonable in all the circumstances to comply with the request without the consent of the third party.

(5) In determining for the purposes of subsection (4)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the third party concerned, regard shall be had, in particular to

(a) any duty of confidentiality owed to the third party;

(b) any steps taken by the data controller with a view to seeking the consent of the third party;

(c) whether the third party is capable of consent; and

(d) any express refusal of consent by the third party.

(6) Where a data controller refuses to comply with a request under this section he shall give reasons in writing for his refusal.

(7) A person aggrieved by the decision of the data controller may appeal to the Commissioner.

(8) Subject to subsection (4), a data controller shall comply with a request under this section within 30 days of the date of receipt of that request.

18. (1) Where the data controller is a credit reference agency, section 9 has effect subject to the provisions of this section.

(2) A person making a request under section 17 may limit his request to personal data relevant to his financial standing, and shall be taken to have so limited his request unless the request shows a contrary intention.

(3) Where the data controller receives a request under section 17 in a case where personal data of which the person making the request is the data subject is being processed by or on behalf of the data controller, the obligation to supply information under that section includes an obligation to give the person making the request a statement, in such a form as may be prescribed by the Minister, of the person's rights.

19. (1) Subject to subsection (2), a data subject is entitled to require the data controller at the end of a 21 day period by notice in writing, to cease, or not begin processing or processing for a specified purpose or in a specified manner, any personal data in respect of which

he is the data subject, on the grounds that,

(a) the processing of that data or the data controller's processing for that purpose or in that manner is causing or is likely to cause substantial damage or distress to the data subject or another; and

(b) damage or distress is or would be unwarranted.

(2) Subsection (1) does not apply

(a) in a case where any of the conditions in paragraphs 1(a) to (b)(iv) of section 6(1); or

(b) in such other cases as may be prescribed by the Minister by Order.

(3) The data controller shall within 21 days of receiving a notice under subsection (1) give the data subject written notice

(a) stating that he has complied or intends to comply with the data subject's notice;

(b) stating reasons for his refusal to comply with a data subject's notice; or

(c) stating the reasons for complying with part of the data subject's notice and the extent of that compliance.

(4) If a court is satisfied, on the application of any data subject who has given notice under subsection (1), that the data controller in question has failed to comply with the notice, the court may order the data controller to take such steps for complying with that notice as the court sees fit.

20. (1) A data subject is entitled at any time by notice in writing to a data controller to require the data controller at the end of a 21 day period to cease, processing for the purposes of direct marketing personal data in respect of which he is the data subject.

(2) If a court is satisfied, on the application of data subject who has given notice under subsection (1), that the data controller has failed to comply with the notice, the court may order data controller to take such steps for complying with the notice as the court sees fit.

(3) For the purposes of this section "indirect marketing" means the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals.

21. (1) An **individual** is entitled at any time, by notice in writing to a data controller, to require the data controller to ensure that no decision is taken by or on behalf of the data which significantly affects that **individual** and is based solely on processing by automatic means of sensitive personal data for the purpose of evaluating matters related to the **individual**

(2) A data controller shall inform a data subject by notice of any decision made by the data controller or on the half of the data controller which is made solely on the processing by automatic means of sensitive personal data for the purpose of evaluating any matters related to that data subject.

(3) The data subject is entitled, within 21 days of receiving that notification from the data controller under subsection (2), by notice in writing to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.

(4) The data controller shall within 21 days of receiving a notice under subsection (3) give the individual a written notice specifying the steps that the data controller intends to take to comply with the data subject's notice.

(5) A notice under subsection (1) does not have effect in relation to an exempt decision; and nothing in subsection (2) applies to an exempt decision.

(6) For the purposes of this section "exempt decision" means any decision

(a) in respect of which the conditions in subsections (7) and (8) are met; or

(b) which is made in such other circumstances as may be prescribed by the Minister.

(7) The condition in this subsection is that the decision

(a) is taken in the course of steps taken

(i) for the purpose of considering whether to enter into a contract with the data subject;

(ii) with a view to entering into such contract;

(iii) in the course of performing such a contract; or

(b) is authorised or required by or under any enactment.

- (8) The condition in this subsection is that either
- (a) the effect of the decision is to grant a request of the data subject; or
 - (b) steps have now been taken to safeguard the legitimate interests of the data subject.

(9) If a court is satisfied, on the application of the data subject that a data controller taking a decision in respect of that data subject has failed to comply with subsection (1) or subsection (2), the court may order the data controller to reconsider the decision, or to take a new decision which is not based solely on processing by automatic means.

22. (1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage.

(2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress where

- (a) the individual also suffers damage by reason of the contravention; or
- (b) the contravention relates to the processing of personal data for
 - (i) the purposes of journalism;
 - (ii) artistic purposes; or
 - (iii) literary purposes.

(3) In proceedings brought against a person by virtue of this section it is a defence to prove that the data controller had taken such care as all the circumstances reasonably required to comply with the requirements concerned.

23. (1) Where a court is satisfied on the application of a data subject that personal data of which the applicant is the subject is inaccurate, the court may order the data controller to rectify, block, erase or destroy those data and any other personal data in respect of which he is the data controller and which contains an expression of opinion which appears to the court to be based on the inaccurate data.

(2) Subsection (1) applies whether or not the data accurately records information received or obtained by the data controller from the data subject or a third party but where the data accurately records such information, where

- (a) the requirements mentioned in section 9 have been complied with, the court may, instead of making an order under subsection (1), make an order requiring the data to be supplemented by such statement of the true facts relating to the matters dealt with by the data as the court may approve; and
- (b) all or any of those requirements have not been complied with, the court may, instead of making an order under that subsection, make such order as it thinks fit for securing compliance with those requirements with or without a further order requiring the data to be supplemented by such a statement as is mentioned in paragraph (a).

(3) Where the court

- (a) makes an order under subsection (1); or
- (b) is satisfied on the application of a data subject that personal data of which he was the data subject and which have been rectified, blocked, erased or destroyed were inaccurate,

it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.

(4) Where a court is satisfied on the application of a data subject

- (a) that he has suffered damage by reason of any contravention by a data controller of any of the requirements of this Act in respect of any personal data, in circumstances entitling him to compensation under section 22; and
- (b) that there is a substantial risk of further contravention in respect of those data in such circumstances,

the court may order the rectification, blocking, erasure or destruction of any of those data.

(5) Where the court makes an order under subsection (4) it may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction.

(6) In determining whether it is reasonably practicable to require such notification as is mentioned in subsection (3) or (5) the court shall have regard, in particular, to the number of persons who would have to be notified.

PART V

REGISTRATION OF DATA CONTROLLERS

24. (1) A person shall not operate as a data controller unless he is registered in the Register of Data Controllers, maintained by the Commissioner and referred to in section 25.

(2) A person who desires to operate as a data controller may

(a) on making an application to the Commissioner in the form prescribed by the Minister; and

(b) on payment to the Commissioner of the prescribed fee

obtain a certificate from the Commissioner for that purpose.

(3) A person who operates without being registered in the manner described under this section shall be liable on summary conviction to pay a fine of \$5 000 or to a term of imprisonment of 2 months or to both.

25. (1) The Commissioner shall keep a register to be known as the Register of Data Controllers in which he shall cause to be entered in relation to the data controller, the following particulars:

(a) the name and address;

(b) the date of registration;

(c) a description of the personal data processed by or on behalf of the data controller and of the category or categories of data subject to which they relate;

(d) a description of the purpose or purposes for which the data is processed;

(e) a description of any recipient or recipients to whom the data controller intends or may wish to disclose the data; and

(f) the names, or a description of, any countries or territories

outside the Caribbean Community to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data.

(2) The Register shall at all reasonable times be open to inspection at the Office **of the Commissioner**.

(3) The Commissioner shall make all amendments to the Register as are necessary.

26. (1) The data controller has a duty to notify the Commissioner of any changes which may affect the particulars entered by the Commissioner in the Register.

(2) A data controller who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$1 000 or to imprisonment for a term of **3 months** and the Commissioner may remove that data controller from the Register.

(3) On receiving notification of the data controller under subsection (1) the Commissioner shall make such amendments to the Register as are necessary.

PART VI

EXEMPTIONS

27. (1) In this Part "the subject information provisions" means

(a) the first data protection principle to the extent to which it requires compliance with section 5(2); and

(b) section 17.

(2) In this part "the non-disclosure provisions" means

(a) the first data protection principle, except to the extent to which it requires compliance with section 6 and section 7;

(b) the second, third, fourth and fifth data protection principles under section 4; and

(c) sections 19 and 23(1) to (3)

to the extent to which they are inconsistent with the disclosure in question.

(3) Except as provided by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorizing the withholding of information.

28. (1) Personal data is exempt from

(a) section 5;

(b) Parts IV and V; and

(c) section 52

where the exemption from **those provisions** is required for the purpose of safeguarding national security.

29. (1) Personal data processed for

(a) the prevention or detection of crime;

(b) the apprehension or prosecution of offenders; or

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

is exempt from the first data protection principle, except to the extent to which it requires compliance with the conditions in section 6, section 7 and section 17 in any case to the extent to which the application of those provisions to the data is likely to prejudice any of the matters mentioned in this subsection.

(2) Personal data which

(a) is processed for the purpose of discharging statutory functions; and

(b) consists of information obtained for such a purpose from a person who had it in his possession for any of the purposes under subsection (1)

is exempt from the subject information provisions to the same extent as personal data processed for any of the purposes under subsection (1).

(3) Personal data is exempt from the non-disclosure provisions in any case in which

(a) the disclosure is for any of the purpose under subsection (1); and

(b) the application of those provisions in relation to disclosure is likely to prejudice any of the matters mentioned under subsection (1).

(4) Personal data in respect of which the data controller is a government department, which

- (a) consist of a classification applied to the data subject as a part of a system of risk assessment which is operated by the relevant authority for
 - (i) the assessment or collection of any tax, duty or of any imposition of a similar nature; or
 - (ii) the prevention or detection of crime, or apprehension or prosecution of offenders, where the offence involves any unlawful claim for payment out of or any unlawful application of public funds; and
- (b) is processed for either of those purposes

is exempt from section 17 to the extent to which the exemption is required in the interests of the operation of the system.

30. (1) The Minister may by Order exempt from the subject information provisions, or modify those provisions in relation to personal data

- (a) consisting of information as to the physical or mental health or condition of a data subject;
- (b) in respect of which the data controller is an educational institution within the meaning assigned to it under section 2 of the *Education Act*, and which consists of information relating to persons who are or have been pupils at the educational institution;
- (c) in respect of which the data controller is a tertiary institution within the meaning assigned to it under section 2 of the *Education Act*, and which consists of information relating to persons who are or have been students at the tertiary institution;
- (d) of other descriptions as may be specified in the Order, being information processed
 - (i) by government departments, public service, charities or other entities designated by or under the Order; and

- (ii) in the course of, or for the purposes of carrying out social work in relation to the data subject

to the extent that the Minister is satisfied that the carrying out of social work is likely to be prejudiced.

31. (1) Personal data processed for the purposes of discharging functions to which this subsection applies is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is designed for the purpose of

- (a) protecting members of the public against
 - (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or 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 authorised to carry on any profession or other activity;
- (b) protecting charities against misconduct or mismanagement, whether by trustees or other persons in their administration;
- (c) protecting the property of charities from loss or misapplication;
- (d) the recovery of the property of charities;
- (e) securing the health, safety and welfare of persons at work; or
- (f) 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.

(3) In subsection (2) "relevant function" means

- (a) any function conferred on any person by or under any

enactment;

- (b) any function of a Minister or government department; or
- (c) any other function which is of a public nature and is exercised in the public interest.

(4) Personal data processed for the purpose of discharging any function which is designed for protecting members of the public against

- (a) maladministration by public bodies;
- (b) failure in services provided by public bodies; or
- (c) a failure of a public body to provide a service which is a function of the body to provide

is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data is likely to prejudice the proper discharge of that function.

(5) Personal data processed for the purpose of discharging any function which is designed for

- (a) protecting members of the public against conduct which may adversely affect their interests by persons carrying on a business;
- (b) 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
- (c) regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market

is exempt from the subject information provisions in any case to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

32. (1) In this section

"research purposes" includes statistical or historical purposes;

"the relevant conditions", in relation to any processing of personal data, means the conditions

- (a) that the data are not processed to support measures or decisions with respect to particular individuals; and
- (b) that the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be caused to any data subject.

(2) For the purposes of the second data protection principle under section 5, the further processing of personal data only for research purposes in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(3) Personal data which are processed only for research purposes in compliance with the relevant conditions may, notwithstanding the fifth data protection principle under section 5, be kept indefinitely.

(4) Personal data which are processed only for research purposes is exempt from section 17 if

- (a) they are processed in compliance with the relevant conditions; and
- (b) the results of the research or any resulting statistics are not made available in a form which identifies data subjects or any of them.

(5) For the purposes of subsections (2) to (4) personal data are not to be treated as processed otherwise than for research purposes merely because the data are disclosed

- (a) to any person, for research purposes only;
- (b) to the data subject or a person acting on his behalf;
- (c) at the request, or with the consent, of the data subject or a person acting on his behalf; or
- (d) in circumstances in which the person making the disclosure has reasonable grounds for believing that the disclosure falls within paragraph (a), (b) or (c).

33. Personal data are exempt from

- (a) the subject information provisions;
- (b) the fourth data protection principle under section 5 and section 22(1) to (3); and
- (c) the non-disclosure provisions

if the data consist of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

34. (1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

(2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary

(a) for the purpose of, or in connection with, any legal proceedings including prospective legal proceedings; or

(b) for the purpose of obtaining legal advice

or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

35. Personal data is exempt from the subject information provisions if the data consists of information in respect of which a claim to legal professional privilege applies.

36. Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs including recreational purposes is exempt from the data protection principles under section 5 and the provisions of Parts IV and V.

37. (1) The Minister may by Order exempt from the subject information provisions personal data consisting of information the disclosure of which is prohibited or restricted by or under any enactment if and to the extent that he considers it necessary for the safeguarding of

(a) the interests of the data subject; or

(b) the rights and freedoms of any other individual

that the prohibition or restriction ought to prevail over those provisions.

(2) The Minister may by Order exempt from the non-disclosure provisions any disclosures of personal data made in circumstances specified in the Order, if he considers the exemption is necessary for the safeguarding of the interests of the data subject or the rights and freedoms of any other person.

PART VII

ENFORCEMENT

38. (1) Where the Commissioner is satisfied that a data controller has contravened or is contravening any of the data protection principles under section 4, the Commissioner may serve him with an enforcement notice requiring him, to do either or both of the following:

- (a) take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified; or
- (b) refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing them for a purpose so specified or in a manner so specified, after such time as may be so specified.

(2) In deciding whether to serve an enforcement notice, the Commissioner shall consider whether the contravention has caused or is likely to cause any person damage or distress.

(3) An enforcement notice in respect of a contravention of the fourth data protection principle which requires the data controller to rectify, block, erase or destroy any inaccurate data may also require the data controller to rectify, block, erase or destroy any other data held by him and containing an expression of opinion which appears to the Commissioner to be based on the inaccurate data.

(4) An enforcement notice in respect of a contravention of the fourth data protection principle under section 4, in the case of data which accurately records information received or obtained by the data controller from the data subject or a third party, may require the data controller either

- (a) to rectify, block, erase or destroy any inaccurate data and any other data held by him and containing an expression of opinion which appears to the Commissioner to be based on inaccurate data; or
- (b) to take such steps as are specified in the notice for securing compliance with the requirements specified in section 9 and, if the Commissioner thinks fit, for supplementing the data with such statement of the true facts relating to the matters dealt with by the data as the Commissioner may approve.

(5) Where

- (a) an enforcement notice requires the data controller to rectify, block, erase or destroy any personal data; or

- (b) the Commissioner is satisfied that personal data which has been rectified, blocked, erased or destroyed had been processed in contravention of any of the data protection principles under section 4,

an enforcement notice may, if reasonably practicable, require the data controller to notify third parties to whom the data has been disclosed of the rectification, blocking, erasure or destruction.

(6) In determining whether it is reasonably practicable to require the notification specified in subsection 5(b) regard shall be had, in particular, to the number of persons who would have to be notified.

(7) An enforcement notice must contain

- (a) a statement of the data protection principle or principles under section 4, which the Commissioner is satisfied have been or are being contravened and his reasons for reaching that conclusion; and

- (b) particulars of the rights of appeal conferred by section 50.

(8) Subject to subsection (9), an enforcement notice shall not require any of the provisions of the notice to be complied with before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(9) Where by reason of special circumstances the Commissioner considers that an enforcement notice should be complied with as a matter of urgency he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion.

(10) Where subsection (8) shall not apply the notice shall not require the provisions of the notice to be complied with before the end of the period of 7 days beginning with the day on which the notice is served.

39. (1) Where the Commissioner considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the data protection principles under section 4, to which it relates, he may cancel or vary the enforcement notice by written notice to the person on whom it was served.

(2) A person on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal can be brought against that enforcement notice, apply in writing to the Commissioner for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the provisions of that notice need not be complied with in order to ensure compliance with the data protection principle or principles under section 4 to which that notice relates.

40. (1) A request may be made to the Commissioner by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data for an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of this Act.

41. (1) Where the Commissioner

(a) has received a request under section 40 in respect of any processing of personal data; or

(b) reasonably requires any information for the purpose of determining whether the data controller has complied or is complying with the data protection principles,

he may serve the data controller with an information notice requiring the data controller, within such time as is specified in the notice, to furnish the Commissioner, in such form as may be so specified, with such information relating to the request or to compliance with the principles as is so specified.

(2) An information notice must contain

(a) in a case falling within subsection (1)(a), a statement that the Commissioner has received a request under section 41 in relation to the specified processing; or

(b) in a case falling within subsection (1)(b), a statement that the Commissioner regards the specified information as relevant for the purpose of determining whether the data controller has complied, or is complying, with the data protection principles and his reasons for regarding it as relevant for that purpose.

(3) An information notice must also contain particulars of the rights of appeal conferred by section 50.

(4) Subject to subsection (5), the time specified in an information notice shall not expire before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(5) Where the Commissioner considers that the information is required as a matter of urgency, he may include in the notice a statement to that effect and a statement of his reasons for reaching that conclusion; and in that event subsection (4) shall not apply, but the notice shall not require the information to be furnished before the end of the period of 7 days beginning with the day on which the notice is served.

(6) A person shall not be required by virtue of this section to furnish the Commissioner with any information in respect of

- (a) any communication between a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act; or
- (b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before the Tribunal) and for the purposes of such proceedings.

(7) In subsection (6) references to the client of a professional legal adviser includes references to any person representing such a client.

(8) A person shall not be required by virtue of this section to furnish the Commissioner with any information if the furnishing of that information would, by revealing evidence of the commission of any offence other than an offence under this Act, expose that person to proceedings for that offence.

(9) The Commissioner may cancel an information notice by written notice to the person on whom it was served.

42. (1) A person who fails to comply with an enforcement notice or an information notice is guilty of an offence, and is liable on summary conviction to pay a fine of \$15 000 or to a term of imprisonment of 6 months.

(2) A person who, in purported compliance with an information notice

- (a) makes a statement which he knows to be false in a material respect; or
- (b) recklessly makes a statement which is false in a material respect, is guilty of an offence.

(3) It is a defence for a person charged with an offence under subsection (1) to prove that he exercised all due diligence to comply with the notice in question.

43. (1) Any notice authorised or required 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 him
 - (i) by delivering it to him;
 - (ii) by sending it to him by post addressed to him at his usual or last known place of residence or business; or
 - (iii) by leaving it for him at that place;

- (b) if that person is a body corporate or partnership, be served
 - (i) by sending it by post to the proper officer of the company at its principal office; or
 - (ii) by addressing it to the proper officer of the partnership and leaving it at the office of the proper officer.

(2) This section is without prejudice to any other lawful method of serving or giving a notice.

44. (1) If a Judge is satisfied by information on oath supplied by the Commissioner that there are reasonable grounds for suspecting

- (a) that a data controller has contravened or is contravening any of the data protection principles, under section 5; or
- (b) 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 Commissioner, the Judge may issue a warrant.

(2) A warrant issued under subsection (1) shall authorise a police officer accompanied by the Commissioner or any of his officers or staff at any time within 7 days of the date of the warrant to enter the premises, to search them, to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data and to inspect and seize any documents or other material found.

45. (1) A police officer executing a warrant may use such reasonable force as may be necessary.

(2) Where the person who occupies the premises in respect of which a warrant issued is present when the warrant is executed, he shall be shown the warrant and supplied with a copy of it; and if that person is not present a copy of the warrant shall be left in a prominent place on the premises.

(3) A police officer seizing anything in pursuance of a warrant shall make a list of any items seized with the date and time of the seizure and shall give the list to the

- (a) data controller; or
- (b) occupier of the premises.

46. (1) The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of personal data which by virtue of section 28 is exempt from any of the provisions of this Act.

(2) Subject to the provisions of this paragraph, the powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of

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

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

47. A warrant issued shall be returned to the court from which it was issued

(a) after being executed; or

(b) if not executed within the time authorised for its execution and the police officer by whom any such warrant is executed shall make an endorsement on it stating what powers have been exercised by him under the warrant.

48. Any person who

(a) intentionally obstructs a person in the execution of a warrant; or

(b) fails without reasonable excuse to give any police officer executing such a warrant such assistance as he may reasonably require for the execution of the warrant, is guilty of an offence and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 12 months or to both.

PART VIII

DATA PROTECTION TRIBUNAL

49. (1) There is established a tribunal called the Data Protection Appeal Tribunal.

(2) The *Second Schedule* has the effect as to the constitution of the Tribunal and otherwise in relation to the Tribunal.

50. (1) A person on whom an enforcement notice or an information notice has been served may appeal to the Tribunal against the notice.

(2) A person on whom an enforcement notice has been served may appeal to the Tribunal against the refusal of an application under section 39(2) for cancellation or variation of the notice.

(3) Where an enforcement notice or an information notice contains a statement by the Commissioner in accordance with section 38(7) or 41(5) then, whether or not the person appeals against the notice, he may appeal against

- (a) the Commissioner's decision to include the statement in the notice; or
- (b) the effect of the inclusion of the statement in respect of any part of the notice.

51. (1) If on an appeal under section 50(1) the Tribunal considers

- (a) that the notice against which the appeal is brought is not in accordance with this Act or any regulations made thereunder; or
- (b) to the extent that the notice involved an exercise of discretion by the Commissioner, and it is determined that the Commissioner ought to have exercised his discretion differently,

the Tribunal shall allow the appeal or substitute such other notice or decision as could have been served or made by the Commissioner and in any other case the Tribunal shall dismiss the appeal.

(2) On such an appeal, the Tribunal may review any determination of fact on which the notice in question was based.

(3) If on an appeal under section 50(2) the Tribunal considers that the enforcement notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal shall cancel or vary the notice.

(4) On an appeal under section 50(3) the Tribunal may direct

- (a) that the notice in question shall have effect as if it did not contain any such statement as is mentioned in that subsection; or
- (b) that the inclusion of the statement in accordance with section 38(7) or 41(5) shall not have effect in relation to any part of the notice, and may make such modifications in the notice as may be required for giving effect to the direction.

(5) On an appeal under section 51(4), the Tribunal may cancel the determination of the Commissioner.

(6) Any party to an appeal to the Tribunal under section 30 may appeal from the decision of the Tribunal on a point of law to the High Court.

PART IX

MISCELLANEOUS

- 52.** (1) A person shall not knowingly or recklessly, without the consent of the data controller
- (a) obtain or disclose personal data or the information contained in personal data; or
 - (b) procure the disclosure to another person of the information contained in personal data.
- (2) Subsection (1) does not apply to a person who shows
- (a) that the obtaining, disclosing or procuring
 - (i) was necessary for the purpose of preventing or detecting crime; or
 - (ii) was required or authorised by or under any enactment, by any rule of law or by the order of a court;
 - (b) that he acted in the reasonable belief that he had in law, the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person;
 - (c) that he acted in the reasonable belief that he would have had the consent of the data controller, if, the data controller had known of the obtaining, disclosing or procuring and the circumstances of it; or
 - (d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.
- (3) A person who, contravenes subsection (1) is guilty of an offence and is liable on summary conviction to pay a fine of \$10 000 or a term of imprisonment of 6 months or to both.
- (4) A person who, sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1) and is liable on summary conviction to pay a fine of \$100 000 or to a term of 3 years or to both.
- (5) A person who, offers to sell personal data is guilty of an offence if
- (a) he has obtained the data in contravention of subsection (1); or
 - (b) he subsequently obtains the data in contravention of subsection (1)

and is liable on summary conviction to pay a fine of \$10 000 or to a term of imprisonment of 2 years or to both.

(6) For the purposes of subsection (5), an advertisement indicating that personal data are or may be for sale is an offer to sell the data.

53. No enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Commissioner or the Tribunal with any information necessary for the discharge of their functions under this Act.

54. (1) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of directors or to be attributable to any neglect on the part of any director, manager, secretary or similar officer of the body corporate or any person who was purporting to act in any such capacity, he as well as the body corporate shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members subsection (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

55. This Act binds the Crown.

56. The Minister may make Regulations generally for the purpose of giving effect to this Act.

57. This Act comes into operation on a date to be fixed by proclamation.

FIRST SCHEDULE

(Section 13(2))

The Data Protection Commissioner

1. (1) The Commissioner shall be appointed by the Minister by instrument in writing from among persons who appear to him to be qualified as having had experience of, and shown capacity in, matters relating to data protection and privacy or such other related discipline.

(2) The Commissioner shall, subject to the provisions of this *Schedule*, hold office for such period not exceeding [3] years as the Minister may specify in the instrument of appointment and shall be eligible for reappointment.

(3) The Minister shall appoint any person appearing to him to have the qualifications necessary for appointment under paragraph 1(2) to act temporarily in the place of the Commissioner in the case of absence or inability to perform the functions of the Commissioner.

2. The Commissioner may at any time resign his office by instrument in writing addressed to the Minister and such resignation shall take effect from the date of the receipt.

3. The Minister shall terminate the appointment of the Commissioner if such Commissioner

- (a) fails to carry out any of the functions conferred or imposed on him under this Act;
- (b) becomes of unsound mind or becomes permanently unable to perform his functions by reason of ill health;
- (c) becomes bankrupt or compounds with, or suspends payment to, his creditors;
- (d) is convicted and sentenced to a term of imprisonment or to death; or
- (e) is convicted of any offence involving dishonesty.

4. The appointment, removal or resignation of a Commissioner shall be notified in the *Gazette*.

SECOND SCHEDULE

(Section 49(2))

Data Protection Appeals Tribunal

Constitution

1. (1) The members of the Tribunal shall be appointed by the Minister by instrument in writing from among persons who appear to him to be qualified as having had experience of, and shown capacity in, matters relating to data protection and privacy or such other related discipline.

(2) The Tribunal shall comprise 5 members who shall be appointed by the Minister.

(3) At least one of the members of the Tribunal shall be an attorney-at-law of at least 10 years standing, and he shall be the Chairman of the Tribunal.

(4) The members of the Tribunal shall hold office for such period not exceeding [3] years as the Minister may specify in the instrument of appointment.

(5) The Minister shall appoint any member of the Tribunal appearing to him to have the qualifications necessary for appointment under paragraph 1(2) to act temporarily in the place of the Chairman in the case of absence or inability to perform the functions of the Chairman.

2. A member of the Tribunal may at any time resign his office by instrument in writing addressed to the Minister and such resignation shall take effect from the date of the receipt.

3. The Minister shall terminate the appointment of any member of the Tribunal where that member

(a) fails to carry out any of the functions conferred or imposed on him under this Act;

(b) becomes of unsound mind or becomes permanently unable to perform his functions by reason of ill health;

(c) becomes bankrupt or compounds with, or suspends payment to, his creditors;

(d) is convicted and sentenced to a term of imprisonment or to death; or

(e) is convicted of any offence involving dishonesty.

4. The appointment, removal or resignation of a member of the Tribunal shall be recorded in the *Official Gazette*.

5. No action, suit, prosecution or other proceedings shall be brought or instituted personally against a member of the Tribunal in respect of any act done *bona fide* in pursuance of their functions under this Act.

6. There shall be paid to the members of the Tribunal such remuneration and other such allowances as the Minister may determine.