

DATA PROTECTION ACT, 2019

OBJECTS AND REASONS

This Bill would

- (a) regulate the collection, keeping, processing, use and dissemination of personal data;
- (b) protect the privacy of individuals in relation to their personal data; and
- (c) provide for matters related to (a) and (b).

DATA PROTECTION ACT, 2019

Arrangement of Sections

PART I

PRELIMINARY

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

PART II

DATA PROTECTION PRINCIPLES

- 4.** Principles relating to processing of personal data
- 5.** Fairness of processing
- 6.** Lawfulness of processing
- 7.** Conditions for consent
- 8.** Conditions applicable to child's consent
- 9.** Processing of sensitive personal data

PART III
RIGHTS OF A DATA SUBJECT

- 10.** Right of access
- 11.** Right to rectification
- 12.** Right to erasure
- 13.** Right to restriction of processing
- 14.** Notification regarding rectification or erasure of personal data or restriction of processing of personal data
- 15.** Right to data portability
- 16.** Right to prevent processing likely to cause damage or distress
- 17.** Right to prevent processing for purposes of direct marketing
- 18.** Automated individual decision-making, including profiling
- 19.** Information to be provided where personal data is collected from the data subject
- 20.** Information to be provided where personal data has not been obtained from the data subject
- 21.** Transparent information, communication and modalities for the exercise of the rights of the data subject

PART IV

TRANSFERS OF PERSONAL DATA OUTSIDE OF BARBADOS

- 22.** General principle for transfers
- 23.** Adequate level of protection
- 24.** Appropriate safeguards
- 25.** Binding corporate rules
- 26.** Derogations
- 27.** Non-compliance
- 28.** Substantial public interest

PART V

EXEMPTIONS

- 29.** References to subject information provisions and non-disclosure provisions
- 30.** National Security
- 31.** Crime and taxation
- 32.** Health, education and social work
- 33.** Regulatory activity
- 34.** Journalism, literature and art
- 35.** Research, history and statistics

- 36.** Manual data held by public authorities
- 37.** Information available to the public by or under enactment
- 38.** Disclosures required by law or made in connection with legal proceedings
- 39.** Parliamentary privilege
- 40.** Legal professional privilege
- 41.** Domestic purposes
- 42.** Confidential references given by the data controller
- 43.** Armed forces
- 44.** Judicial appointments and honours
- 45.** Appointments to public service
- 46.** Corporate finance
- 47.** Negotiations with data subject
- 48.** Examinations
- 49.** Powers to make further exemptions by order

PART VI

DATA CONTROLLER AND DATA PROCESSOR

- 50.** Data controllers must be registered
- 51.** Register of Data Controllers

- 52.** Notification of changes in respect of a data controller
- 53.** Responsibility of the data controller
- 54.** Data protection by design and by default
- 55.** Data processors must be registered
- 56.** Register of Data Processors
- 57.** Notification of changes in respect of a data processor
- 58.** Data Processor
- 59.** Processing under the authority of the data controller or data processor
- 60.** Records of processing activities
- 61.** Cooperation with the Commissioner
- 62.** Security of processing
- 63.** Notification of a personal data breach to the Commissioner
- 64.** Communication of a personal data breach to the data subject
- 65.** Data protection impact assessment
- 66.** Prior consultation
- 67.** Designation of the data privacy officer
- 68.** Position of the data privacy officer
- 69.** Duties and functions of a data privacy officer

PART VII
DATA PROTECTION COMMISSIONER

70. Data Protection Commissioner

71. Functions of Commissioner

72. Staff

73. Confidential information

74. Indemnity

75. Report

PART VIII
ENFORCEMENT

76. Enforcement notice

77. Cancellation of enforcement notice

78. Request for assessment

79. Information notice

80. Special information notice

81. Determination by Commissioner as to the purposes of journalism or artistic or literary purposes

82. Restriction on enforcement in case of processing for the purposes of journalism or for artistic or literary purposes

- 83.** Failure to comply with notice
- 84.** Service of notice by Commissioner
- 85.** Warrants
- 86.** Execution of warrants
- 87.** Matters exempt from inspection and seizure
- 88.** Return of warrants
- 89.** Obstruction of execution of a warrant

PART IX

DATA PROTECTION TRIBUNAL

- 90.** Establishment of the Data Protection Tribunal
- 91.** Right of appeal
- 92.** Determination of appeals

PART X

MISCELLANEOUS

- 93.** Right to compensation and liability
- 94.** Unlawful obtaining of personal data
- 95.** Administrative penalty
- 96.** Disclosure of information

97. Act binds Crown

98. Amendment of *Schedule*

99. Regulations

100. Commencement

SCHEDULE

Data Protection Tribunal

BARBADOS

A Bill entitled

An Act to

- (a) regulate the collection, keeping, processing, use and dissemination of personal data;
- (b) protect the privacy of individuals in relation to their personal data; and
- (c) provide for matters related to (a) and (b).

ENACTED by the Parliament of Barbados as follows:

PART I

PRELIMINARY

Short title

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

Interpretation

2. In this Act

“accessible public record” means any record that is kept by a public authority and 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;

“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allow or confirm the unique identification of that individual;

“child” means a person who is under the age of 18 years;

“Commissioner” means the Data Protection Commissioner referred to in section 70;

“consent” in relation to a data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him;

“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;
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record; or
- (e) does not fall within paragraph (a), (b), (c) or (d) but is recorded information held by a public authority;

“data controller” means

- (a) a person who alone, jointly or in common with others determines the purposes for which, and the manner in which, any personal data is or should be processed; or
- (b) where personal data is processed only for the purpose for which the data is required by or under an enactment to be processed, the person on whom the obligation to process the data is imposed by or under an enactment;

“data privacy officer” means a person designated as such pursuant to section 67;

“data processor” means any person, other than an employee of a data controller, who processes personal data on behalf of the data controller;

“data subject” means an individual who is the subject of personal data;

“genetic data” means personal data relating to the inherited or acquired genetic characteristics of an individual which gives unique information about the physiology or the health of that individual and which result, in particular, from an analysis of a biological sample from the individual;

“health care professional” includes a person who is registered under

- (a) the *Medical Professions Act* (Act 2011-1);
- (b) the *Dental Registration Act*, Cap. 367;
- (c) the *Nurses Act*, Cap. 372 or enrolled under that Act;
- (d) the *Pharmacy Act*, Cap. 372D; and
- (e) the *Paramedical Professions Act*, Cap. 372C;

“health record” means any record which

- (a) consists of information relating to the physical or mental condition of an individual; and
- (b) has been made by or on behalf of a health care professional in connection with the care of the individual;

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

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

“personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

“process” in relation to information or data, means to obtain, record or hold the information or data or carry out any operation or set of operations on the information or data, including the

- (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;

“profiling” means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

“pseudonymisation” means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable individual;

“public authority” means a public office or a ministry, department, agency, unit other authority of the Government including a statutory body;

“recipient” means a person, public authority, agency or another body, to which the personal data is disclosed but a public authority shall not be considered a recipient where the personal data is received pursuant to an obligation imposed by the any enactment;

“relevant filing system” means any set of information relating to individuals to the extent that although the information 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 relating to a particular individual is readily accessible;

“representative” means a representative of the data controller or data processor who is not established in Barbados and is nominated pursuant to

- (a) section 50(3) in respect of a data controller; or

(b) section 55(3) in respect of a data processor

and who represents that data controller or data processor with regard to their obligations under this Act;

“restriction of processing of personal data” means the marking of stored personal data with the aim of limiting their processing in the future;

“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 a political body;

(e) membership of a trade union;

(f) genetic data;

(g) biometric data;

(h) sexual orientation or sexual life;

(i) financial record or position;

(j) criminal record; or

(k) proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings;

“trade union” has the meaning assigned to it by the *Trade Unions Act, Cap. 361*;

“Tribunal” means the Data Protection Tribunal established pursuant to section 90.

Application of Act

- 3.(1) This Act applies to
- (a) the processing of personal data in the context of the activities of a data controller or a data processor established in Barbados;
 - (b) the processing of personal data of data subjects in Barbados by a data controller or a data processor not established in Barbados, where the processing activities are related to the offering of goods or services to data subjects in Barbados.
- (2) For the purposes of subsection (1) “established in Barbados” means
- (a) an individual who is ordinarily resident in Barbados;
 - (b) a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
 - (c) a person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to the processing of personal data.

PART II

DATA PROTECTION PRINCIPLES

Principles relating to processing of personal data

- 4.(1) Personal data shall be
- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject;
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
 - (d) accurate and, where necessary, kept up to date and every reasonable step shall be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
 - (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
 - (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- (2) A data controller shall, in relation to all of the personal data he processes, comply with the requirements set out in subsection (1).
- (3) A data controller may specify the purpose for which personal data is obtained pursuant to subsection 1(b)
- (a) in any notice given for the purposes of section 5(3)(a) by the data controller to the data subject; or
 - (b) in a notification given to the Commissioner pursuant to Part III.
- (4) In determining whether any disclosure of personal data is compatible with the purpose for which the data is obtained in accordance with subsection 1(b), regard is to be had to the purpose for which the personal data is intended to be processed by any person to whom the data is disclosed.

(5) Subsection 1(d) is not 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 was obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and
- (b) 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.

(6) Pursuant to subsection 1(f), 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; and
- (b) the nature of the data to be protected.

(7) The data controller shall take reasonable steps to ensure that his employees who have access to the personal data comply with the requirements set out in subsection (1).

(8) Pursuant to subsection 1(f), where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall

- (a) choose a data processor who provides 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 the measures referred to in paragraph (a).

(9) 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 subsection 1(f) 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 subsection 1(f).

(10) A person who fails to comply with the requirements set out in subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to imprisonment for 3 years or to both.

Fairness of processing

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

(2) Subject to subsection (3), personal data is to be treated as having been obtained fairly if the personal data consists of information obtained from a person who is

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

- (3) Personal data is 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 readily available to him, the following information:
 - (i) the identity of the data controller;
 - (ii) where a data controller has nominated a representative for the purposes of this Act, the identity of that representative;
 - (iii) the purpose or purposes for which the data is intended to be processed; and
 - (iv) any further information which is necessary, having regard to the specific circumstances in which the data is or is 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 is provided with, or has readily available to him, the information specified in subparagraphs (i) to (iv) of paragraph (a).
- (4) For the purposes of subsection (3)(b), “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 is in fact disclosed to such a person within that period, the time when the data is first disclosed;
 - (ii) if within that period the data controller becomes, or ought to become aware that the data is 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.

Lawfulness of processing

6.(1) Processing shall be lawful where

- (a) the data subject has given consent to the processing of his personal data for one or more specific purposes; or
- (b) the processing is necessary
 - (i) for the performance of a contract to which the data subject is a party;
 - (ii) for the taking of steps at the request of the data subject with a view to entering into a contract;
 - (iii) for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
 - (iv) in order to protect the vital interests of the data subject;
 - (v) for the administration of justice;
 - (vi) for the exercise of any functions of either House of Parliament;
 - (vii) for the exercise of any functions conferred on any person by or under any enactment;
 - (viii) for the exercise of any functions of a public authority;
 - (ix) for the purposes of legitimate interests pursued by the data controller or by the third party to whom the data is 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; or
 - (x) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which

require protection of personal data, in particular where the data subject is a child.

(2) Subsection (1)(b)(x) shall not apply to processing carried out by public authorities in the performance of their tasks.

Conditions for consent

7.(1) Where processing is based on consent, the data controller shall demonstrate that the data subject has consented to processing of his personal data.

(2) Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

(3) A data subject has the right to withdraw his consent in respect of the processing of his personal data at any time and the data controller shall inform the data subject of his right to withdraw prior to him giving consent to the data controller to process his personal data.

(4) The withdrawal of consent by the data subject shall not affect the lawfulness of processing based on consent before its withdrawal.

(5) In determining whether consent is freely given, the data controller shall take into account whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Conditions applicable to child's consent

8.(1) The processing of a child's personal data shall be lawful only where and to the extent that consent is given or authorised by the parent or guardian of the child.

(2) The data controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the parent or guardian of a child, taking into consideration available technology.

(3) Subsection (1) shall not affect contract law under any enactment in respect of the validity, formation or effect of a contract in relation to a child.

Processing of sensitive personal data

9.(1) Processing of sensitive personal data shall be prohibited unless

- (a) the data subject gives his consent to the processing;
- (b) the processing 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;
- (c) the processing 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;
- (d) the processing 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;
- (e) the processing
 - (i) is carried out in the course of its legitimate activities by any body or association which
 - (A) is not established or conducted for profit; and
 - (B) exists for political, philosophical, religious or trade union purposes;
 - (ii) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
 - (iii) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and

- (iv) does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (f) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;
- (g) the processing is necessary
 - (i) for the purpose of, or in connection with, any legal proceedings including prospective legal proceedings;
 - (ii) for the purpose of obtaining legal advice; or
 - (iii) otherwise for the purposes of establishing, exercising or defending legal rights;
- (h) the processing is necessary for the administration of justice;
- (i) the processing is necessary for the exercise of any functions of either House of Parliament;
- (j) the processing is necessary for the exercise of any functions conferred on any person by or under an enactment;
- (k) the processing is necessary for the exercise of any functions of a public authority;
- (l) the processing is necessary for medical purposes and is undertaken by
 - (i) a health care professional; or
 - (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 care professional;
- (m) the processing
 - (i) is of sensitive personal data consisting of information as to racial or ethnic origin; and
 - (ii) 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

- (iii) is carried out with appropriate safeguards for the rights and freedoms of data subjects.
- (2) The Minister may by order specify circumstances other than those identified in subsection (1) where sensitive personal data may be processed.
- (3) An order made pursuant to subsection (2) is subject to negative resolution.
- (4) For the purposes of subsection (1)(l) “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health care services.

PART III

RIGHTS OF A DATA SUBJECT

Right of access

- 10.(1)** A data subject has the right
- (a) to be informed by a data controller whether personal data of that 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 from, and to be given by, the data controller, a description of
 - (i) the purposes of the processing;
 - (ii) the categories of personal data concerned;
 - (iii) the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in other countries or international organisations;

- (iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- (v) the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- (vi) the right to lodge a complaint with the Commissioner;
- (vii) any available information as to their source, where the personal data is not collected from the data subject;
- (viii) the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(2) Where personal data is transferred to another country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to section 24.

(3) The data controller shall provide a copy of the personal data undergoing processing to the data subject and where more copies are requested by the data subject, the data controller may charge a reasonable fee based on administrative costs.

(4) Where the data subject makes the request for personal data by electronic means, and unless otherwise requested by the data subject, the personal data shall be provided in electronic form.

(5) The right of the data subject to obtain a copy of personal data referred to subsection (3) shall not adversely affect the rights and freedoms of other data subjects.

Right to rectification

11.(1) The data subject shall have the right to obtain from the data controller, without undue delay, the rectification of inaccurate personal data concerning him.

(2) Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed by the data controller, including by means of providing a supplementary statement.

Right to erasure

12.(1) The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him without undue delay.

(2) The data controller shall erase personal data, without undue delay, where one of the following grounds applies

- (a) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- (b) the data subject withdraws consent where the processing is done pursuant to section 6(1)(a) or section 9(1)(a), and where there is no other legal ground for the processing;
- (c) the data subject objects to the processing pursuant to section 16 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to section 17;
- (d) the personal data has been unlawfully processed;
- (e) the personal data has to be erased in compliance with a legal obligation in Barbados to which the data controller is subject.

(3) Where the data controller has made the personal data public and is obliged pursuant to subsection (1) or (2) to erase the personal data, the data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data controllers who are processing the personal data that the data subject has requested the erasure

by such data controllers of any links to, or copy or replication of, the personal data.

(4) Subsections (1), (2) and (3) shall not apply to the extent that processing is necessary

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires processing by any enactment to which the data controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- (c) for reasons of public interest in the area of public health;
- (d) for archiving for the purposes of research, history or statistics in accordance with section 35; or
- (e) for the establishment, exercise or defence of legal claims.

Right to restriction of processing

13.(1) The data subject shall have the right to obtain from the data controller restriction of processing of personal data where one of the following applies:

- (a) the accuracy of the personal data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the personal data;
- (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- (c) the data controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- (d) the data subject has objected to processing pursuant to section 16 pending the verification whether the legitimate grounds of the data controller override those of the data subject.

(2) Where processing has been restricted under subsection (1), the personal data shall, with the exception of storage, only be processed

- (a) with the data subject's consent;
- (b) for the establishment, exercise or defence of legal claims;
- (c) for the protection of the rights of another person; or
- (d) for reasons of important public interest of Barbados.

(3) A data subject who has obtained restriction of processing of personal data pursuant to subsection (1) shall be informed by the data controller before the restriction of processing of personal data is removed pursuant to subsection (2).

Notification regarding rectification or erasure of personal data or restriction of processing of personal data

14.(1) The data controller shall communicate any

- (a) rectification of personal data pursuant to section 11;
- (b) erasure of personal data pursuant to section 12; or
- (c) restriction of processing of personal data pursuant to section 13

to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.

(2) The data controller shall inform the data subject about those recipients where the data subject requests such information.

Right to data portability

15.(1) The data subject has the right to receive the personal data concerning him, which he has provided to a data controller, in a structured, commonly used and machine-readable format.

(2) The data subject has the right to transmit the personal data concerning him, which he has provided to a data controller to another data controller without hindrance where

- (a) the processing is based on consent pursuant to section 6(1)(a) or section 9(1)(a) or on a contract pursuant to section 6(1)(b)(i); and
- (b) the processing is carried out by automated means.

(3) In exercising his right to data portability pursuant to subsections (1) and (2), the data subject shall have the right to have his personal data transmitted directly from one data controller to another, where technically feasible.

(4) The exercise of the right referred to in subsection (1) shall be exercised without prejudice to section 12.

(5) The exercise of the right referred to in subsection (1) shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.

(6) The exercise of the right referred to in subsection (1) shall not adversely affect the rights and freedoms of other data subjects.

Right to prevent processing likely to cause damage or distress

16.(1) Subject to subsection (2), a data subject is entitled, by a written notice, to require the data controller at the end of a 21 day period to cease, or not to 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 ground that

- (a) the processing of the 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) the damage or distress is or would be unwarranted.

(2) Subsection (1) does not apply

- (a) in a case where any of the conditions in section 6(1)(a) or (b)(i), (ii), (iii) or (iv) is satisfied; or
- (b) in such other cases as the Minister may prescribe by order.

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

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

(4) Where the High Court is satisfied, on the application of a 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 the notice as the Court sees fit.

Right to prevent processing for purposes of direct marketing

17.(1) A person is entitled at any time, by a written notice 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) Where the High Court is satisfied, on the application of a data subject who has given notice under subsection (1), that the data controller has failed to comply with the notice, the Court may order the data controller to take such steps for complying with the notice as the Court sees fit.

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

Automated individual decision-making, including profiling

18.(1) The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or similarly significantly affects him.

(2) Subsection (1) shall not apply where the automated processing or profiling of personal data is

- (a) necessary for entering into, or performance of, a contract between the data subject and a data controller;
- (b) authorised by any enactment to which the data controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- (c) based on the data subject's consent.

(3) In the cases referred to in subsection (2)(a) and (c), the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.

(4) Subsection (2) shall not apply to sensitive personal data unless it is in the public interest and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

Information to be provided where personal data is collected from the data subject

19.(1) Where personal data relating to a data subject is collected from the data subject, the data controller shall, at the time when personal data is obtained, provide the data subject with the following:

- (a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- (b) the contact details of the data privacy officer, where applicable;

- (c) the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
 - (d) where the processing is done pursuant to 6(1)(b)(x), the legitimate interests pursued by the data controller or by a third party;
 - (e) the recipients or categories of recipients of the personal data, if any;
 - (f) where applicable, the fact that the data controller intends to transfer personal data to another country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers to the appropriate safeguards referred to in section 24 and the means by which to obtain a copy of them or where they have been made available.
- (2) In addition to the information referred to in subsection (1), the data controller shall at the time when personal data is obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:
- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
 - (b) the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
 - (c) where the processing is done pursuant to section 6(1)(a) or section 9(1)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
 - (d) the right to lodge a complaint with the Commissioner;
 - (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well

as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data was collected, the data controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in subsection (2).

(4) Subsections (1), (2) and (3) shall not apply where the data subject already has the information.

Information to be provided where personal data has not been obtained from the data subject

20.(1) Where personal data has not been obtained from the data subject, the data controller shall provide the data subject with the following:

- (a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- (b) the contact details of the data privacy officer, where applicable;
- (c) the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- (d) the categories of personal data concerned;
- (e) the recipients or categories of recipients of the personal data, if any;
- (f) where applicable, that the data controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers to the appropriate safeguards referred to in

section 24 Parliamentary Counsel and the means to obtain a copy of them or where they have been made available.

(2) In addition to the information referred to in subsection (1), the data controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

- (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- (b) where the processing is done pursuant to section 6(1)(b)(x), the legitimate interests pursued by the data controller;
- (c) the existence of the right to request from the data controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
- (d) where processing is done pursuant to section 6(1)(a) or section 9(1)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (e) the right to lodge a complaint with the Commissioner;
- (f) from the source from which originated the personal data, and if applicable, whether it came from publicly accessible sources;
- (g) the existence of automated decision-making, including profiling, referred to in section 18 and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(3) The data controller shall provide the information referred to in subsections (1) and (2)

- (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data is processed;

- (b) if the personal data is to be used for communication with the data subject, at the latest, at the time of the first communication to that data subject; or
 - (c) if a disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed.
- (4) Where the data controller intends to further process the personal data for a purpose other than that for which the personal data was obtained, the data controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in subsection (2).
- (5) Subsections (1), (2), (3) and (4) shall not apply where and insofar as:
- (a) the data subject already has the information;
 - (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes pursuant to section 35;
 - (c) obtaining or disclosure is expressly laid down by any enactment to which the data controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
 - (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by any enactment.

Transparent information, communication and modalities for the exercise of the rights of the data subject

21.(1) The data controller shall take appropriate measures to provide any information referred to in section 19 and section 20 and any communication under sections 10 to 18 and section 63 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

- (2) The information pursuant to subsection (1) shall be provided in writing, or by other means, including, where appropriate, by electronic means.
- (3) When requested by the data subject, the data controller may provide the information, pursuant to his rights under sections 10 to 15 and 18 orally, provided that the identity of the data subject is verified.
- (4) The data controller shall facilitate the exercise of data subject rights under sections 10 to 15 and 18.
- (5) The data controller shall provide information on action taken on a request under sections 10 to 15 and 18 to the data subject without undue delay and in any event within one month of receipt of the request.
- (6) The period of time referred to in subsection (5) shall be extended by two months where necessary, taking into account the complexity and number of the requests under sections 10 to 15 and 18.
- (7) The data controller shall inform the data subject of any extension granted pursuant to subsection (6) within one month of receipt of the request, together with the reasons for the delay.
- (8) Where the data subject makes the request pursuant to his rights under sections 10 to 15 and 18 by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
- (9) Where the data controller does not take action on the request of the data subject under this section, the data controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Commissioner or appealing to the High Court.
- (10) Information provided under section 18 and section 19 and any communication and any actions taken under sections 10 to 15 and 18 and section 63 shall be provided free of charge.

(11) Where requests referred to in this section from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the data controller may either

- (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- (b) refuse to act on the request.

(12) The data subject may object to the decision of a data controller made pursuant to subsection (11) by lodging a complaint with the Commissioner or appealing to the Tribunal.

(13) For the purposes of subsection (12), the data controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of a request referred to in subsection (11).

(14) Where a data controller has reasonable doubts concerning the identity of the individual making a request pursuant to sections 10 to 18, the data controller may request the provision of additional information necessary to confirm the identity of the data subject.

(15) The information to be provided to data subjects pursuant to section 19 and section 20 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing and where the icons are presented electronically they shall be machine-readable.

(16) The Minister in consultation with the Commissioner, may make regulations for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

PART IV

TRANSFERS OF PERSONAL DATA OUTSIDE OF BARBADOS

General principle for transfers

22. Personal data shall not be transferred to a country or territory outside Barbados unless that country or territory provides for

- (a) an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of their personal data; and
- (b) appropriate safeguards on condition that the rights of the data subject are enforceable and there are available, effective legal remedies for data subjects.

Adequate level of protection

23. For the purposes of section 22, 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 is 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.

Appropriate safeguards

24. For the purposes of section 22, appropriate safeguards may be provided for by

- (a) a legally binding and enforceable instrument between public authorities;
- (b) binding corporate rules in accordance with section 25;
- (c) standard data protection clauses prescribed by the Commissioner with the approval of the Minister;
- (d) contractual clauses authorised by the Commissioner between the data controller or data processor and the data controller, data processor or the recipient of the personal data; or
- (e) provisions, authorised by the Commissioner, to be inserted into administrative arrangements between public authorities which include enforceable and effective data subject rights.

Binding corporate rules

25.(1) Data controllers and data processors shall develop binding corporate rules which shall specify

- (a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;
- (b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;
- (c) their legally binding nature, both in and outside of Barbados;

- (d) the application of principles regarding purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of sensitive personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;
- (e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with this Act, the right to lodge a complaint with the competent supervisory authority or Commissioner and the High Court and to obtain any other available form of redress and, where appropriate, compensation for a breach of the binding corporate rules;
- (f) the acceptance by the data controller or data processor of liability for any breaches of the binding corporate rules;
- (g) that the data controller or the data processor shall be exempt from the liability referred to in paragraph (f), in whole or in part, only where it is proven that the data controller or data processor is not responsible for the event giving rise to the damage;
- (h) how the information on the binding corporate rules is provided to the data subjects;
- (i) the complaint procedures;
- (j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules;
- (k) the mechanisms for reporting and recording changes to the binding corporate rules and reporting those changes to the supervisory authority;
- (l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of

enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority or Commissioner the results of verifications of the measures specified in paragraph (j);

- (m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- (n) the appropriate data protection training to personnel having permanent or regular access to personal data.

(2) The binding corporate rules referred to in subsection (1) shall be submitted to the Commissioner for authorisation.

(3) The Commissioner may specify the format and procedures for the exchange of information between data controllers, data processors and supervisory authorities for binding corporate rules.

(4) For the purposes of this section,

“binding corporate rules” means personal data protection policies which are adhered to by a data controller or data processor for transfers or a set of transfers of personal data to a data controller or a data processor in one or more countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;

“enterprise” means a person engaged in an economic activity;

“group of undertakings” means a controlling undertaking and its controlled undertakings;

“supervisory authority” means an independent public authority which is established by in a country or territory outside of Barbados.

Derogations

26. Section 22, 23 and 24 shall not apply where

- (a) the data subject has given his consent to the transfer of personal data;
- (b) the transfer of personal data 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 interest of the data subject;
 - (iv) the performance of a contract described in subparagraph (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 of personal data 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 is or may be disclosed after the transfer;

- (d) the transfer of personal data 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 of personal data 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.

Non-compliance

27. A person who contravenes sections 22, 23 or 24 is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to imprisonment for 3 years or to both.

Substantial public interest

28.(1) The Minister may by order specify the

- (a) circumstances in which a transfer of the personal data of data subjects outside of Barbados is to be considered to be necessary for reasons of substantial public interest; and
- (b) circumstances in which a transfer of the personal data of data subjects outside of Barbados, which is not required by or under an enactment, is not to be considered necessary for reasons of substantial public interest.

(2) An order made pursuant to subsection (1) shall be subject to negative resolution.

PART V

EXEMPTIONS

References to subject information provisions and non-disclosure provisions

29.(1) In this Part

- (a) “the subject information provisions” refers to
 - (i) section 4(1)(a) to the extent to which it requires compliance with section 5(2); and
 - (ii) section 10;
- (b) “the non-disclosure provisions” refers to the following provisions to the extent to which they are inconsistent with the disclosure in question:
 - (i) section 4(1)(a), except to the extent to which it requires compliance with the conditions in 6 and 9;
 - (ii) section 4(1) (b), (c), (d), (e); and
 - (iii) sections 11 to 18.

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

National Security

30. Parts II, III, IV, VI and section 79 do not apply where the processing of the personal data is required for the purpose of safeguarding national security.

Crime and taxation

31.(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 other imposition of a similar nature,

is exempt from section 4(1)(a), except to the extent to which it requires compliance with the conditions in section 6 and 9, and from section 10 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 paragraphs (a) to (c).

(2) Personal data which

- (a) is processed for the purpose of discharging statutory functions; and
- (b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in subsection (1)(a) to (c)

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

(3) Personal data is exempt from the non-disclosure provisions where

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

(4) Personal data in respect of which the data controller is a public authority and 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 public authority for any of the following purposes:
 - (i) the assessment or collection of any tax, duty or other imposition of a similar nature; or

- (ii) the prevention or detection of crime or the apprehension or prosecution of offenders, where the offence concerned involves an unlawful claim for payment out of, or an unlawful application of, public funds; and
- (b) is processed for either of those purposes

is exempt from section 10 to the extent to which the exemption is required in the interests of the operation of the system.

Health, education and social work

32.(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 and which consist 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 and which consist of information relating to persons who are or have been students at the tertiary institution;
- (d) of such other descriptions as may be specified in the order, being information processed
 - (i) by public authorities, 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 or other individuals.

(2) Notwithstanding subsection (1)(d), Minister shall not confer any exemption or make any modification under subsection (1)(d) except so far as he

considers that the application to the data of those provisions (or of those provisions without modification) is likely to prejudice the carrying out of social work.

(3) In subsection (1)

“educational institution” has the meaning assigned to it by section 2 of the *Education Act*, Cap. 41;

“tertiary institution” has the meaning assigned to it by section 2 of the *Education Act*, Cap. 41.

Regulatory activity

33.(1) Personal data processed for the purposes of discharging functions to which this subsection applies is exempt from the subject information provisions 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) Personal data processed for the purpose of discharging any function which is designed for protecting members of the public against

- (a) maladministration by public authorities;
- (b) failures in services provided by public authorities; or
- (c) a failure of a public authority to provide a service which it is a function of the authority 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 would be likely to prejudice the proper discharge of that function.

(4) 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 to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of that function.

- (5) For the purposes of subsection (2) “relevant function” means
- (a) any function conferred on any person by or under any enactment;
 - (b) any function of a public authority; or
 - (c) any other function which is of a public nature and is exercised in the public interest.

Journalism, literature and art

34.(1) Personal data which is processed only for the purposes of journalism or for artistic or literary purposes is exempt from any provision to which this subsection relates where

- (a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material;
- (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest; and
- (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the purpose of journalism or artistic or literary purposes.

(2) In considering for the purposes of subsection (1)(b) whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to his compliance with any code of practice which is relevant to the publication in question and is designated by the Minister by order for the purposes of this subsection.

(4) In any proceedings against a data controller where the data controller claims, or it appears that any personal data to which the proceedings relate are being processed

- (a) only for the purposes of journalism or for artistic or literary purposes; and

(b) with a view to the publication by any person of any journalistic, literary or artistic material which, at the time 24 hours immediately before the relevant time, had not previously been published by the data controller, the proceedings shall be stayed until either of the conditions in subsection (5) is met.

(5) The conditions referred to in subsection (4) are

- (a) that a determination of the Commissioner with respect to the data in question takes effect; or
- (b) in a case where the proceedings were stayed on the making of a claim, that the claim is withdrawn.

(6) For the purposes of this section “publication”, in relation to journalistic, literary or artistic material, means make available to the public or any section of the public.

Research, history and statistics

35.(1) The 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 it was obtained.

(2) Personal data which is processed only for research purposes in compliance with the relevant conditions may be kept indefinitely.

(3) Personal data which is processed only for research purposes is exempt from section 10 where

- (a) the personal data is 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.

(4) For the purposes of subsections (1) to (3), personal data is not to be treated as processed otherwise than for research purposes merely because the data is 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).

(5) In this section

“research purposes” includes statistical or historical purposes;

“the relevant conditions”, in relation to processing of personal data, means the conditions that the data

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

Manual data held by public authorities

36. Personal data which fall within paragraph (e) of the definition of “data” in section 2 is exempt from Parts II, III, IV and VI.

Information available to the public by or under enactment

37. Personal data is exempt from Parts II, III, IV and VI where 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.

Disclosures required by law or made in connection with legal proceedings

38.(1) Personal data is 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 of competent jurisdiction.

(2) Personal data is 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.

Parliamentary privilege

39. Personal data is exempt from Parts II, III, IV and VI where the exemption is required for the purpose of avoiding an infringement of the privileges of either House of Parliament.

Legal professional privilege

40. Personal data is exempt from the subject information provisions where the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.

Domestic purposes

41. 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 Parts II, III, IV and VI.

Confidential references given by the data controller

42. Personal data is exempt from section 10 where it consists of a reference given or to be given in confidence by the data controller for the purposes of

- (a) the education, training or employment, or prospective education, training or employment, of the data subject;
- (b) the appointment, or prospective appointment, of the data subject to any office; or
- (c) the provision, or prospective provision, by the data subject of any service.

Armed forces

43. Personal data is exempt from the subject information provisions to the extent to which the application of those provisions would be likely to prejudice the combat effectiveness of any of the armed forces of the Crown.

Judicial appointments and honours

44. Personal data processed for the purposes of

- (a) assessing any person's suitability for judicial office or the office of Queen's Counsel; or
- (b) the conferring by the Crown of any honour or dignity,

is exempt from the subject information provisions.

Appointments to public service

45. The Minister may by order exempt from the subject information provisions personal data processed for the purposes of assessing any person's suitability for

- (a) employment in the Public Service; or

- (b) any office to which appointments are made by the Governor-General or by a Minister.

Corporate finance

46.(1) Where personal data is processed for the purposes of, or in connection with, a corporate finance service

- (a) the data is exempt from the subject information provisions to the extent to which either
 - (i) the application of those provisions to the data could affect the price of any instrument which is already in existence or is to be or may be created; or
 - (ii) the data controller reasonably believes that the application of those provisions to the data could affect the price of any such instrument; and
 - (b) to the extent that the data is not exempt from the subject information provisions by virtue of paragraph (a), the data is exempt from those provisions where the exemption is required for the purpose of safeguarding an important economic or financial interest of Barbados.
- (2) For the purposes of subsection (1)(b) the Minister may by order specify
- (a) matters to be taken into account in determining whether exemption from the subject information provisions is required for the purpose of safeguarding an important economic or financial interest of Barbados; or
 - (b) circumstances in which exemption from those provisions is, or is not, to be taken to be required for that purpose.
- (3) In this section

“corporate finance service”means a service consisting of

- (a) underwriting in respect of issues of, or the placing of issues of, any instrument;
- (b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings; or
- (c) services relating to such underwriting as is mentioned in paragraph (a);

“price”includes value.

Negotiations with data subject

47. Personal data which consist of records of the intentions of the data controller in relation to any negotiations with the data subject is exempt from the subject information provisions in any case to the extent to which the application of those provisions would be likely to prejudice those negotiations.

Examinations

48.(1) The results of an examination are exempt from section 10.

(2) Personal data consisting of information recorded by candidates during an academic, professional or other examination is exempt from section 10.

(3) In this section “examination” includes any process for determining the knowledge, intelligence, skill or ability of a candidate by reference to his performance in any test, work or other activity.

Powers to make further exemptions by order

49.(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 where 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, where 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.

(3) An order made under this section shall be subject to negative resolution.

PART VI

DATA CONTROLLER AND DATA PROCESSOR

Data controllers must be registered

50.(1) A person shall not operate as a data controller unless he is registered in the Register of Data Controllers.

(2) A person who desires to operate as a data controller may, upon application to the Commissioner in the prescribed form and payment of the prescribed fee, obtain a certificate from the Commissioner for the purpose.

(3) A data controller that is not established in Barbados shall nominate, for the purposes of this Act, a representative established in Barbados.

(4) A person who operates as a data controller without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(5) A data controller who is not established in Barbados and who does not nominate a representative pursuant to subsection (3) is guilty of an offence and

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

(6) For the purposes of subsections (3) and (5), each of the following is to be treated as established in Barbados:

- (a) an individual who is ordinarily resident in Barbados;
- (b) a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
- (c) any person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing.

Register of Data Controllers

51.(1) The Commissioner shall keep a register, to be called the Register of Data Controllers, in which he shall cause to be entered in relation to each data controller registered pursuant to section 50, the following particulars:

- (a) the name and address and other contact information of the data controller;
- (b) the date of registration;
- (c) a description of the personal data processed by or on behalf of the data controller and of the categories of data subject to which they relate;
- (d) a description of the purposes for which the data is processed;
- (e) a description of any recipients to whom the data controller intends or may wish to disclose the data;
- (f) the names, or a description of, any countries outside Barbados to which the data controller directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data; and

- (g) where the data controller is not established in Barbados within the meaning of section 50(6), the name, address and other contact information of the representative nominated pursuant to section 50(3).
- (2) The Register of Data Controllers shall be open to inspection at the office of the Commissioner.
- (3) The Commissioner shall ensure that the Register of Data Controllers is kept accurate and up to date.

Notification of changes in respect of a data controller

- 52.(1)** The data controller shall give written notice to the Commissioner of any changes which may affect the particulars entered in the Register of Data Controllers in relation to him.
- (2) On receiving notification of the data controller under subsection (1) the Commissioner shall make such amendments to the Register of Data Controllers as are necessary.

Responsibility of the data controller

- 53.(1)** The data controller shall implement the appropriate technical and organisational measures to ensure that processing is performed in accordance with this Act taking into consideration the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity to the rights and freedoms of individuals.
- (2) Where proportionate in relation to processing activities, the measures referred to in subsection (1) shall include the implementation of appropriate data protection policies by the data controller.

Data protection by design and by default

- 54.(1)** The data controller shall both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement the

principles set out in section 4 in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Act and protect the rights of data subjects, taking into consideration the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.

(2) The data controller shall implement the appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing is processed.

(3) Subsection (2) applies to the amount of personal data collected, the extent of processing of the personal data, the period of storage of the personal data and the accessibility to the personal data.

(4) The technical and organisational measures referred to in subsection (1) shall ensure that personal data is not, by default, made accessible without the individual's intervention to an indefinite number of individuals.

Data processors must be registered

55.(1) A person shall not operate as a data processor unless he is registered in the Register of Data Processors.

(2) A person who desires to operate as a data processor may, upon application to the Commissioner in the prescribed form and payment of the prescribed fee, obtain a certificate from the Commissioner for the purpose.

(3) A data processor that is not established in Barbados shall nominate, for the purposes of this Act, a representative established in Barbados.

(4) A person who operates as a data processor without being registered under subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$10 000 or to a term of imprisonment of 2 months or to both.

(5) A data processor that is not established in Barbados and who does not nominate a representative pursuant to subsection (3) is guilty of an offence and

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

(6) For the purposes of subsections (3) and (5), each of the following is to be treated as established in Barbados:

- (a) an individual who is ordinarily resident in Barbados;
- (b) a body, association or other entity incorporated, organised, registered or otherwise formed under any enactment; or
- (c) any person who does not fall within paragraph (a) or (b) but maintains in Barbados an office, branch or agency through which he carries on any activity related to data processing.

Register of Data Processors

56.(1) The Commissioner shall keep a register, to be called the Register of Data Processors, in which he shall cause to be entered in relation to each data processor, the following particulars:

- (a) the name and address and other contact information of the data processor;
- (b) the date of registration;
- (c) a description of the personal data processed by or on behalf of the data processor and of the categories of data subject to which they relate;
- (d) a description of the purposes for which the data is processed;
- (e) a description of any recipients to whom the data processor intends or may wish to disclose the data;
- (f) the names, or a description of, any countries or territories outside Barbados to which the data processor directly or indirectly transfers, or intends or may wish directly or indirectly to transfer, the data; and

- (g) where the data processor is not established in Barbados within the meaning of section 55(6), the name, address and other contact information of the representative nominated pursuant to section 55(3).
- (2) The Register of Data Processors shall be open to inspection at the office of the Commissioner.
- (3) The Commissioner shall ensure that the Register of Data Processors is kept accurate and up to date.

Notification of changes in respect of a data processor

- 57.(1)** The data processor shall give written notice to the Commissioner of any changes which may affect the particulars entered in the Register of Data Processors in relation to him.
- (2) On receiving notification of the data processor under subsection (1) the Commissioner shall make such amendments to the Register of Data Processors as are necessary.

Data Processor

- 58.(1)** Where processing is to be carried out on behalf of a data controller, the data controller shall only use a data processor who shall implement the appropriate technical and organisational measures to ensure that processing will
- (a) be in accordance with the requirements of this Act; and
 - (b) ensure the protection of the rights of the data subject.
- (2) The data processor shall not engage another data processor without prior specific or general written authorisation of the data controller.
- (3) Where there is general written authorisation pursuant to subsection (2), the data processor shall inform the data controller of any intended changes concerning the addition or replacement of other data processors and the data controller shall be given the opportunity to object to such changes.

(4) Processing by a data processor shall be governed by a written contract between the data processor and the data controller which sets out the following:

- (a) the subject-matter and duration of the processing;
- (b) the nature and purpose of the processing;
- (c) the type of personal data and categories of data subjects;
- (d) the obligations and rights of the data controller.

(5) The contract prepared pursuant to subsection (4) shall also stipulate that the data processor

- (a) processes the personal data only on documented instructions from the data controller, including with regard to transfers of personal data to countries outside of Barbados or an international organisation, unless required to do so by any enactment and in such a case, the data processor shall inform the data controller of that legal requirement before processing, unless the enactment prohibits such information to be shared on important grounds of public interest;
- (b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- (c) takes all measures required pursuant to section 62.
- (d) respects the conditions referred to in subsections (2) and (7) for engaging another data processor;
- (e) taking into account the nature of the processing, assists the data controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the data controller's obligation to respond to requests for exercising the data subject's rights under Part III;

- (f) assists the data controller in ensuring compliance with the obligations pursuant to sections 62 to 66 taking into account the nature of processing and the information available to the data processor;
- (g) on the determination of the data controller, deletes or returns all the personal data to the data controller after the end of the provision of services relating to processing, and deletes existing copies unless the enactment requires storage of the personal data;
- (h) makes available to the data controller all information necessary to demonstrate compliance with the obligations set out in this section and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

(6) Where in relation to subsection (5)(h) an instruction from the data controller to the data processor infringes this Act, the data processor shall immediately inform the data controller.

(7) Where a data processor engages another data processor for carrying out specific processing activities on behalf of the data controller in accordance with subsection (2), the same obligations as set out in the contract between the data controller and the data processor as referred to subsections (5) and (6) shall be imposed on that other data processor, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Act.

(8) Where that other data processor mentioned in subsection (7) fails to fulfil its data protection obligations, the initial data processor referred to in subsection (7) shall remain fully liable to the data controller for the performance of that other data processor's obligations.

(9) The Commissioner with the approval of the Minister may prescribe standard contractual clauses for the matters referred to in subsections (5) and (7).

(10) Where data processor contravenes this Act by determining the purposes and means of processing, the data processor shall be considered to be a data controller in respect of that processing.

Processing under the authority of the data controller or data processor

59.(1) The data processor and any person acting under the authority of the data controller or of the data processor, who has access to personal data, shall not process those data except on instructions from the data controller, unless required to do so by any enactment.

(2) A person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction to a fine of \$500 000 or to a term of imprisonment of 3 years or to both.

Records of processing activities

60.(1) A data controller and, where applicable, the data controller's representative, shall maintain a record of processing activities under its responsibility and that record shall contain all of the following:

- (a) the name and contact details of the data controller and, where applicable, the joint data controller, the data controller's representative and the data privacy officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;
- (d) the categories of recipients to whom the personal data has been or will be disclosed including recipients in other countries or international organisations;
- (e) where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in section 26, the documentation of suitable safeguards;
- (f) where possible, the envisaged time limits for erasure of the different categories of data;

- (g) where possible, a general description of the technical and organisational security measures referred to in section 62(1).
- (2) A data processor and, where applicable, the data processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a data controller, which contains:
- (a) the name and contact details of the data processor or data processors and of each data controller on behalf of whom the data processor is acting, and, where applicable, of the data controller's or the data processor's representative, and the data privacy officer;
 - (b) the categories of processing carried out on behalf of each data controller;
 - (c) where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in section 26, the documentation of suitable safeguards;
 - (d) where possible, a general description of the technical and organisational security measures referred to in section 62(1).

Cooperation with the Commissioner

61. A data controller and the data processor and, where applicable, their representatives, shall cooperate, on request, with the Commissioner in the performance of his tasks.

Security of processing

62.(1) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, the data controller and the data processor shall implement appropriate technical and

organisational measures to ensure a level of security appropriate to the risk, including:

- (a) the pseudonymisation and encryption of personal data;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

(2) In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

(3) The data controller and data processor shall take steps to ensure that any individual acting under the authority of the data controller or the data processor who has access to personal data does not process the personal data except on instructions from the data controller, unless he is required to do so by any enactment.

Notification of a personal data breach to the Commissioner

63.(1) Where there is a personal data breach the data controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Commissioner, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

(2) Where the notification of the personal data breach to the Commissioner is not made within 72 hours, the notification shall be accompanied by reasons for the delay.

(3) The data processor shall notify the data controller without undue delay after becoming aware of a personal data breach.

(4) The notification of the personal data breach to the Commissioner referred to in subsection (1) shall

- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the data privacy officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach;
- (d) describe the measures taken or proposed to be taken by the data controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

(5) Where it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

(6) The data controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken in order to facilitate the Commissioner in his assessment of the data controller's compliance with this section.

Communication of a personal data breach to the data subject

64.(1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the data controller shall communicate the personal data breach to the data subject without undue delay and, where feasible, not later than 72 hours after having become aware of it.

(2) The communication to the data subject referred to in subsection (1) shall describe in clear and plain language the nature of the personal data breach and

contain the information referred to in paragraphs (b), (c) and (d) of section 63(4).

(3) The communication to the data subject referred to in subsection (1) shall not be required where any of the following conditions are met:

- (a) the data controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- (b) the data controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in subsection (1) is no longer likely to materialise;
- (c) it would involve disproportionate effort and in such a case, there shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Data protection impact assessment

65.(1) Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of an individual, the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) A single assessment pursuant to subsection (1) may address a set of similar processing operations that present similar high risks.

(3) The data controller shall seek the advice of the data privacy officer, where designated, when carrying out a data protection impact assessment.

(4) A data protection impact assessment referred to in subsection (1) shall in particular be required in the case of:

- (a) a systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning an individual or similarly significantly affect the individual;
- (b) processing on a large scale of sensitive personal data; or
- (c) a systematic monitoring of a publicly accessible area on a large scale.

(5) The Commissioner shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to subsection (1) and the Commissioner shall publish that list in the *Official Gazette*.

(6) The Commissioner shall establish and make public a list of the kind of processing operations where no data protection impact assessment is required and the Commissioner shall publish that list in the *Official Gazette*.

(7) A data protection impact assessment referred to in subsection (1) shall contain

- (a) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in subsection (1); and
- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act taking into account

the rights and legitimate interests of data subjects and other persons concerned.

(8) Where appropriate, the data controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

(9) Where necessary, the data controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Prior consultation

66.(1) The data controller shall consult the Commissioner prior to processing where a data protection impact assessment under section 65 indicates that the processing would result in a high risk to the rights and freedoms of an individual in the absence of measures taken by the data controller to mitigate the risk.

(2) Where the Commissioner is of the opinion that the intended processing referred to in subsection (1) would infringe this Act, in particular where the data controller has insufficiently identified or mitigated the risk, the Commissioner shall, within a period of up to 8 weeks of receipt of the request for consultation, provide written advice to the data controller and, where applicable to the data processor.

(3) The period mentioned in subsection (2) may be extended by 6 weeks, taking into account the complexity of the intended processing.

(4) The Commissioner shall inform the data controller and, where applicable, the data processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay.

(5) The period mentioned in subsection (2) may be suspended until the Commissioner has obtained information he has requested for the purposes of the consultation.

(6) When consulting the Commissioner pursuant to subsection (1), the data controller shall provide the Commissioner with:

- (a) where applicable, the respective responsibilities of the data controller and data processors involved in the processing, in particular for processing within a group of undertakings;
- (b) the purposes and means of the intended processing;
- (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Act;
- (d) where applicable, the contact details of the data privacy officer;
- (e) the data protection impact assessment provided for in section 65;
- (f) any other information requested by the Commissioner.

Designation of the data privacy officer

67.(1) The data controller and the data processor shall designate a data privacy officer in any case where:

- (a) the processing is carried out by a public authority or body, except for a court of competent jurisdiction acting in their judicial capacity;
- (b) the core activities of the data controller or the data processor consist of processing operations which, by virtue of their nature, their scope and their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- (c) the core activities of the data controller or the data processor consist of processing on a large scale of sensitive personal data.

(2) A group of undertakings may appoint a single data privacy officer provided that a data privacy officer is easily accessible from each establishment.

(3) Where a data controller or the data processor is a public authority or body, a single data privacy officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

(4) In cases other than those referred to in subsection (1), the data controller or data processor or associations and other bodies representing categories of data controllers or data processors may designate a data privacy officer.

(5) The data privacy officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the duties and functions referred to in section 69.

(6) The data privacy officer may be a staff member of the data controller or data processor, or fulfil the tasks on the basis of a service contract.

(7) The data controller or the data processor shall communicate the contact details of the data privacy officer to the Commissioner.

Position of the data privacy officer

68.(1) The data controller and the data processor shall ensure that the data privacy officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

(2) The data controller and data processor shall support the data privacy officer in performing the duties and functions referred to in section 69 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his expert knowledge.

(3) A data privacy officer shall not be dismissed or penalised by the data controller or the data processor for performing duties and functions referred to in section 69.

(4) A data privacy officer shall report directly to highest management level of a data controller or a data processor.

(5) Data subjects may contact the data privacy officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Act.

(6) A data privacy officer is required to keep confidential all matters concerning the performance of his duties and functions referred to in section 69.

Duties and functions of a data privacy officer

- 69.(1)** A data privacy officer shall
- (a) inform and advise the data controller or the data processor and the employees who carry out processing of their obligations pursuant to this Act;
 - (b) monitor compliance with this Act and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
 - (c) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section 65;
 - (d) cooperate with the Commissioner;
 - (e) act as the contact point for the Commissioner on issues relating to processing, including the prior consultation referred to in section 66, and to consult, where appropriate, with regard to any other matter.
- (2) A data privacy officer shall in the performance of his duties and functions under this section have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

PART VII

DATA PROTECTION COMMISSIONER

Data Protection Commissioner

70.(1) There shall be a public officer, to be called the Data Protection Commissioner, who shall be responsible for the general administration of this Act.

(2) A person is qualified to hold or to act in the post of Data Protection Commissioner, where that person is qualified to practise as an attorney-at- law and has so practised for a period of not less than 7 years, or for periods amounting in the aggregate to not less than 7 years.

(3) In this section “practise as an attorney-at-law” includes any period during which a person served as an attorney-at-law, advocate, barrister-at-law, solicitor, parliamentary counsel, magistrate or registrar of a court of competent jurisdiction in some part of the Commonwealth, or as a professor or teacher of law at the University of the West Indies or at a school for legal education approved by the Judicial and Legal Service Commission.

Functions of Commissioner

71. Without prejudice to the generality of the functions set out in this Act, the functions of the Commissioner are to

- (a) monitor and enforce the application of this Act;
- (b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;
- (c) promote the awareness of data controllers and data processors of their obligations under this Act;
- (d) organise activities addressed specifically to children to educate them about the risks, rules, safeguards and rights in relation to processing;

- (e) conduct, at his own discretion or where requested to do so by any person, an audit of the personal data processed by the person, for the purpose of ascertaining whether or not the data is processed in accordance with this Act;
 - (f) upon request, provide information to any data subject concerning the exercise of their rights under this Act;
 - (g) monitor the processing of personal data and, in particular, sensitive personal data, and any other matter affecting the privacy of persons in respect of their personal data, and
 - (i) report to the Minister on the results of that monitoring; and
 - (ii) where appropriate, make recommendations on the need for, or desirability of, taking legislative, administrative or other action to give protection or better protection, to the privacy of persons in respect of their personal data;
 - (h) examine any proposed legislation or proposed policy of the Government that
 - (i) the Commissioner considers may affect the privacy of persons in respect of their personal data; or
 - (ii) provides for the collection of personal data by any public authority or the disclosure of personal data by one public authority to another public authority,
- and report to the Minister the results of that examination;
- (i) conduct investigations on the application of this Act, including on the basis of information received from a public authority;
 - (j) receive and invite representations from members of the public on any matter affecting the privacy of persons in respect of their personal data;

- (k) consult and cooperate with other persons concerned with the privacy of persons in respect of their personal data;
- (l) 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 interest of the privacy of persons in respect of their personal data;
- (m) provide, at his own discretion or where requested to do so, advice to any Minister, public authority or person on any matter relevant to the operation of this Act;
- (n) inquire generally into any matter, including any law, practice or procedure, whether governmental or non-governmental, or any technical development, where it appears to the Commissioner that the privacy of persons in respect of their personal data is being or may be infringed thereby;
- (o) undertake research into, and monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons in respect of their personal data is minimised, and report to the Minister the results of such research and monitoring;
- (p) report to the Minister on the desirability of the acceptance, by Barbados, of any international instrument relating to the privacy of persons in respect of their personal data;
- (q) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- (r) prepare appropriate codes of practice for the guidance of persons processing personal data;
- (s) recommend the adoption and development of standard contractual clauses and standard data protection clauses pursuant to this Act;

- (t) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to section 65(5) and (6);
- (u) investigate complaints from persons concerning abuses in the processing of personal data;
- (v) approve binding corporate rules pursuant to section 25;
- (w) keep internal records of contraventions of this Act and of measures taken to address those contraventions;
- (x) do anything incidental or conducive to the performance of any of the preceding functions; and
- (y) exercise such other functions as are conferred or imposed on the Commissioner by or under this Act or any other enactment.

Staff

72.(1) There shall be appointed to assist the Commissioner in the discharge of his functions such number of public officers as may be required.

(2) A person appointed pursuant to subsection (1) section is subject to the Commissioner's direction and control in the performance of functions under this Act.

Confidential information

73.(1) The Commissioner and a public officer appointed pursuant to section 72(1) shall keep secret all confidential information coming to his knowledge during the course of the administration of this Act or any other Act that the Commissioner has jurisdiction to administer or enforce, except insofar as disclosure is necessary for the administration of this Act or insofar as the Commissioner authorises that person to release the information.

(2) Subsection (1) shall not apply where disclosure is required pursuant to

- (a) an order made by a court of competent jurisdiction;
- (b) a duty or obligation imposed by any enactment; or

(c) an international agreement to which Barbados is a party.

(3) A person who contravenes subsection (1) subject to subsection (2) is guilty of an offence and is liable on summary conviction to a fine of \$50 000 or to imprisonment for a term of 12 months, or to both.

(4) In this section, “confidential information” means information of any kind and in any form that relates to one or more persons and that is obtained by or on behalf of the Commissioner for the purpose of administering or enforcing this Act or any enactment that the Commissioner has jurisdiction to administer or enforce, or that is prepared from such information, but does not include information that does not directly or indirectly reveal the identity of the person to whom it relates.

Indemnity

74. The Commissioner and his staff shall not be subject to any action, claim or demand by, or liability to, any person in respect of anything done or omitted to be done in good faith in the discharge or in connection with the discharge of the functions conferred on the Commissioner and his staff pursuant to this Act.

Report

75.(1) The Commissioner shall, not later than 3 months after the end of each financial year, submit to the Minister a report of the activities and operations of the Commissioner throughout the preceding financial year in such detail as the Minister may direct.

(2) A copy of the report of the Commissioner referred to in subsection (1) shall be printed and laid before both Houses of Parliament and published in the Official Gazette not later than 3 months from the date of receipt thereof by the Minister.

PART VIII

ENFORCEMENT

Enforcement notice

76.(1) Where the Commissioner is satisfied that a data controller or a data processor has contravened or is contravening this Act, the Commissioner may serve him with a notice, to be referred to as an “enforcement notice” requiring him, to do either or both of the following:

- (a) to 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) to refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing the personal data 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 shall contain

- (a) a statement of the provision of the Act which the Commissioner is satisfied have been or are being contravened and his reasons for reaching that conclusion; and
- (b) particulars of the right of appeal conferred by section 91.

(4) Subject to subsections (5) and (6), 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, where such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(5) 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.

(6) Where subsection (5) applies, 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.

Cancellation of enforcement notice

77.(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 this Act, 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 the notice on the ground that, by reason of a change of circumstances, all or any of the provisions of the notice need not be complied with in order to ensure compliance with the provisions of this Act to which the notice relates.

Request for assessment

78.(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 this Act.

(2) On receiving a request under this section, the Commissioner shall make an assessment in such manner as appears to him to be appropriate, unless he is not supplied with such information as he may reasonably require to

- (a) satisfy himself as to the identity of the person making the request; and

(b) enable him to identify the processing in question.

(3) The matters to which the Commissioner may have regard in determining in what manner it is appropriate to make an assessment include

- (a) the extent to which the request appears to him to raise a matter of substance;
- (b) any undue delay in making the request; and
- (c) whether or not the person making the request has a right to access the personal data in question as specified in section 10.

(4) Where the Commissioner has received a request under this section he shall notify the person who made the request

- (a) whether he has made an assessment as a result of the request; and
- (b) to the extent that he considers appropriate, having regard in particular to any exemption from section 10 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request.

Information notice

79.(1) Where the Commissioner

- (a) has received a request under section 78 in respect of any processing of personal data; or
- (b) reasonably requires any information for the purpose of determining whether a data controller has complied or is complying with the data protection principles,

he may serve the data controller with a notice, to be referred to as an “information notice”, requiring the data controller to furnish him with specified information relating to the request or to compliance with the provisions of this Act.

(2) An information notice shall contain

(a) in a case falling within

- (i) subsection (1)(a), a statement that the Commissioner has received a request under section 78 in relation to the specified processing; or
- (ii) subsection (1)(b), a statement that the Commissioner regards the specified information as relevant for the purpose of determining whether the data controller or the data processor has complied or is complying with the provisions of this Act and his reasons for regarding it as relevant for that purpose; and

(b) particulars of the right of appeal conferred by section 91.

(3) The Commissioner may specify in an information notice

- (a) the form in which the information must be furnished; and
- (b) the period within which, or the time and place at which, the information must be furnished.

(4) Subject to subsection (5), a period specified in an information notice under subsection (3)(b) must not end, and a time so specified must not fall, before the end of the period within which an appeal can be brought against the notice and, where such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(5) Where by reason of special circumstances 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 where the furnishing of that information would, by revealing evidence of the commission of any offence, other than an offence under this Act or an offence of perjury, expose that person to proceedings for that offence.

(9) Any relevant statement provided by a person in response to a requirement under this section may not be used in evidence against that person on a prosecution for an offence under this Act, other than an offence under section 83, unless in the proceedings

- (a) in giving evidence the person provides information that is inconsistent with it; and
- (b) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

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

(11) This section has effect subject to section 82(3).

- (12) In subsection (1) “specified information” means information
- (a) specified or described in the information notice; or
 - (b) falling within a category which is specified or described in the information notice.
- (13) In subsection (9), “relevant statement”, in relation to a requirement under this section, means
- (a) an oral statement; or
 - (b) a written statement made for the purposes of the requirement.

Special information notice

- 80.(1)** Where the Commissioner
- (a) receives a request under section 78 in respect of any processing of personal data; or
 - (b) has reasonable grounds for suspecting that, in a case in which proceedings have been stayed under section 34, the personal data to which the proceedings relate
 - (i) is not being processed only for the purposes of journalism or for artistic or literary purposes; or
 - (ii) is not being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller,

he may serve the data controller with a notice, referred to as a “special information notice”, requiring the data controller to furnish him with specified information for the purpose specified in subsection (2).

- (2) The purpose referred to in subsection (1) is the purpose of ascertaining whether personal data is being processed

- (a) only for the purposes of journalism or for artistic or literary purposes; or

- (b) with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller.
- (3) A special information notice must contain
- (a) particulars of the right of appeal conferred by section 91; and
 - (b) in a case falling within
 - (i) subsection (1)(a), a statement that the Commissioner has received a request under section 78 in relation to the specified processing; or
 - (ii) subsection (1)(b), a statement of the Commissioner's grounds for suspecting that the personal data is not being processed as mentioned in that paragraph.
- (4) The Commissioner may also specify in the special information notice
- (a) the form in which the information must be furnished; and
 - (b) the period within which, or the time and place at which, the information must be furnished.
- (5) Subject to subsection (6), a period specified in a special information notice under subsection (4)(b) must not end, and a time so specified must not fall, 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.
- (6) Where by reason of special circumstances 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 (5) 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.

(7) 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.

(8) In subsection (7) a reference to the client of a professional legal adviser include a reference to any person representing such a client.

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

(10) Any relevant statement provided by a person in response to a requirement under this section may not be used in evidence against that person on a prosecution for any offence under this Act, other than an offence under section 83, unless in the proceedings

- (a) in giving evidence the person provides information inconsistent with it; and
- (b) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

(11) In subsection (10) “relevant statement”, in relation to a requirement under this section, means

- (a) an oral statement; or
- (b) a written statement made for the purposes of the requirement.

(12) The Commissioner may cancel a special information notice by written notice to the person on whom it was served.

(13) In subsection (1) “specified information”means information

- (a) specified, or described, in the special information notice; or
- (b) falling within a category which is specified, or described, in the special information notice.

Determination by Commissioner as to the purposes of journalism or artistic or literary purposes

81.(1) Where at any time it appears to the Commissioner, whether as a result of the service of a special information notice or otherwise, that any personal data is not being processed

- (a) only for the purposes of journalism or for artistic or literary purposes; or
- (b) with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller,

he may make a determination in writing to that effect.

(2) Notice of the determination shall be given to the data controller; and the notice must contain particulars of the right of appeal conferred by section 91.

(3) A determination under subsection (1) shall not take effect until the end of the period within which an appeal can be brought and, where an appeal is brought, shall not take effect pending the determination or withdrawal of the appeal.

Restriction on enforcement in case of processing for the purposes of journalism or for artistic or literary purposes

82.(1) The Commissioner may not serve an enforcement notice on a data controller with respect to the processing of personal data for the purposes of journalism or for artistic or literary purposes unless

- (a) a determination under section 81(1) with respect to those data has taken effect; and
- (b) the High Court has granted leave for the notice to be served.

(2) The High Court shall not grant leave for the purposes of subsection (1) (b) unless he is satisfied

- (a) that the Commissioner has reason to suspect a contravention of the data protection principles which is of substantial public importance; and
- (b) except where the case is one of urgency, that the data controller has been given notice of the application for leave.

(3) The Commissioner may not serve an information notice on a data controller with respect to the processing of personal data for the purposes of journalism or for artistic or literary purposes unless a determination under section 81(1) with respect to those data has taken effect.

Failure to comply with notice

83.(1) A person who fails to comply with an enforcement notice, an information notice or a special information notice is guilty of an offence and is liable on summary conviction to 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 and is liable on summary conviction to a fine of \$500 000 or to a term of imprisonment of 3 years or to both.

(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.

Service of notice by Commissioner

84.(1) Any notice authorised or required by this Act to be served on or given to any person by the Commissioner may where the person is

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

(3) Nothing in subsections (1) and (2) precludes the service of a notice by electronic means.

Warrants

85.(1) Where a Judge of the High Court is satisfied by information on oath supplied by the Commissioner that there are reasonable grounds for suspecting that

- (a) a data controller or a data processor has contravened or is contravening Parts II, III or IV; or
- (b) an offence under this Act has been or is being committed, and that evidence of the contravention or of the commission of the offence is to be found on any premises specified by the Commissioner,

the Judge may issue a warrant.

(2) A warrant issued, under subsection (1), shall authorise a police officer accompanied by the Commissioner, staff or such other person skilled in information technology as the police officer may deem necessary for the purpose, within 7 days of the date of the warrant, to

- (a) enter the premises;
- (b) search the premises;
- (c) inspect, examine, operate and test any equipment found on the premises which is used or intended to be used for the processing of personal data;
- (d) inspect and seize any documents or other material found on the premises;
- (e) require any person on the premises to provide
 - (i) an explanation of any document or other material found on the premises;
 - (ii) such other information as may reasonably be required for the purpose of determining whether the data controller has contravened or is contravening Parts II, III or IV.

(3) A Judge shall not issue a warrant in respect of any personal data processed for the purposes of journalism or for artistic or literary purposes unless a determination by the Commissioner under section 81 with respect to those data has taken effect.

Execution of warrants

86.(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 is issued is present when the warrant is executed, he shall be shown the warrant and supplied with a copy of it and where the 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

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

Matters exempt from inspection and seizure

87.(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 30, is exempt from any of the provisions of this Act.

(2) The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of any communication between

- (a) 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) 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.

Return of warrants

88. A warrant shall be returned to the High Court

- (a) after being executed; or
- (b) where 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.

Obstruction of execution of a warrant

89. Any person who

- (a) intentionally obstructs a person in the execution of a warrant;
- (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;
- (c) makes a statement in response to a requirement under section 85(2)(e) which that person knows to be false in a material respect; or
- (d) recklessly makes a statement in response to a requirement under section 85(2)(e) which is false in a material respect,

is guilty of an offence and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 2 years or to both.

PART IX

DATA PROTECTION TRIBUNAL

Establishment of the Data Protection Tribunal

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

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

Right of appeal

91.(1) A person on whom an enforcement notice, an information notice or a special 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 77(2) for cancellation or variation of the notice.

(3) Where an enforcement notice, an information notice or a special information notice contains a statement by the Commissioner in accordance with section 76(3), section 79(5) or 80(6) 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.

(4) A data controller in respect of whom a determination has been made under section 81 may appeal to the Tribunal against the determination.

(5) A person on whom an order has been made pursuant to under section 94 may appeal to the Tribunal against that order.

Determination of appeals

92.(1) Where on an appeal under section 91(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) Upon appeal pursuant to subsection (1), the Tribunal may review any determination of fact on which the notice in question was based.

(3) Where on an appeal under 91(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 91(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 76(3), section 79(5) or 80(6) 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 91(4), the Tribunal may cancel the determination of the Commissioner.

(6) Any party to an appeal to the Tribunal under section 91 may appeal from the decision of the Tribunal on a point of law to the High Court.

PART X

MISCELLANEOUS

Right to compensation and liability

93.(1) An individual who suffers damage or distress due to any contravention of this Act by the data controller or the data processor is entitled to compensation from that data controller or the data processor for that damage.

(2) In proceedings brought by an individual pursuant to subsection (1), it is a defence for the data controller or the data processor to prove that he took all such measures in the circumstances as would be reasonably required to comply with the provisions of this Act.

Unlawful obtaining of personal data

94.(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 that

- (a) 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 of competent jurisdiction;
- (b) 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) 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) 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 a fine of \$10 000 or to a term of imprisonment of 6 months or to both.

(4) A person who sells personal data is guilty of an offence if he obtained the data in contravention of subsection (1) and is liable on summary conviction to a fine of \$100 000 or to a term of imprisonment of 3 years or to both.

(5) A person who offers to sell personal data is guilty of an offence where

- (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 a fine of \$100 000 or to a term of imprisonment of 3 years or to both.

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

Administrative penalty

95.(1) Where the Commissioner after a hearing determines that a person has contravened section 52(1), section 57(1) and sections 60 to 67 and the Commissioner considers it to be in the public interest to make an order, the Commissioner may order the person to pay to the Crown a penalty of an amount not exceeding \$50 000.

(2) In addition to the public interest, where the Commissioner seeks to make an order pursuant to subsection (1), he shall have due regard to the following:

- (a) the nature, gravity and duration of the contravention taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
- (b) the intentional or negligent character of the contravention;
- (c) any action taken by the data controller or data processor to mitigate the damage suffered by data subjects;
- (d) any relevant previous contraventions by the data controller or data processor;
- (e) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the contravention;
- (f) the categories of personal data affected by the contravention;
- (g) the manner in which the contravention became known to the Commissioner and, in particular whether, and to what extent, the data controller or data processor gave notice of the contravention; and
- (h) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the contravention.

(3) Where the Commissioner makes an order under subsection (1) the Commissioner shall file in the registry of the High Court a copy of the order certified by the Commissioner, and on being filed the order shall have the same force and effect, and all proceedings may be taken on it, as if it were a judgment of the High Court, unless an appeal has been filed pursuant to section 91.

(4) A penalty imposed by the Commissioner in the exercise of his powers under this Act shall be payable into the general revenue and may be recovered by the Crown as a civil debt and for the purposes of the proof of such debt a

certificate under the hand of the Commissioner shall be receivable in evidence as sufficient proof of such debt.

(5) A person aggrieved by an order made by the Commissioner pursuant to subsection (1) may appeal to the Tribunal within 28 days of the date of the order.

Disclosure of information

96. 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.

Act binds Crown

97. This Act binds the Crown.

Amendment of *Schedule*

98. The Minister may by order amend the *Schedule*.

Regulations

99. The Minister may make Regulations generally for the purposes of giving effect to this Act.

Commencement

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

SCHEDULE*(Section 90)**Data Protection Tribunal**Constitution***Members of the Tribunal**

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 a person appearing to him to have the qualifications necessary for appointment under paragraph 1(3) to act temporarily in the place of the Chairman where the Chairman is absent or unable to perform his functions.

Resignation

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 by the Minister of that instrument.

Revocation of appointments

3. The Minister shall revoke 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.

Gazetting appointments

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

Protection of the members of the Tribunal

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 in good faith in pursuance of their functions under this Act.

Remuneration of the members of the Tribunal

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

Read three times and passed the House of Assembly this
day of , 2019.

Speaker

Read three times and passed the Senate this day of
 , 2019.

President

PARLIAMENT

FIRST SESSION OF 2018-2023

BILL

cited as the Data Protection Act,
2019

Government Printing Department