The Official Gazette

(EXTRAORDINARY)

OF GUYANA

Published by the Authority of the Government

GEORGETOWN, WEDNESDAY 19TH JULY, 2023

TABLE OF CONTENTS **PAGE**

FIRST SUPPLEMENT

LEGAL SUPPLEMENT

A. **ACTS — NIL**

B. **SUBSIDIARY LEGISLATION — NIL**

C. **BILLS —** BILL No. 14 of 2023 – The Data Protection Act 2023 423

GEORGETOWN, Demerara – Printed and Published every Saturday and on such Extraordinary Days as may be directed by the Government by Guyana National Printers Limited, 1 Public Road, La Penitence, Greater Georgetown.

THE OFFICIAL GAZETTE 19TH JULY, 2023
LEGAL SUPPLEMENT — C

BILL No. 14 of 2023

Wednesday 19th July, 2023

PARLIAMENT OFFICE
Public Buildings,
Georgetown,
Guyana.

19th July, 2023.

The following Bill which will be introduced in the National Assembly is published for general information.

S.E. Isaacs,
Clerk of the National Assembly.

GUYANA

BILL NO. 14 OF 2023

DATA PROTECTION BILL 2023

ARRANGEMENT OF SECTIONS

SECTION

PART I
PRELIMINARY

1. Short title.
2. Interpretation.
3. Scope 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 of consent.
8. Conditions applicable to a child's consent.
9. Processing of sensitive personal data.
10. Processing which does not require identification.

PART III

RIGHTS OF A DATA SUBJECT

11. Rights of access.
12. Right to rectification.
13. Right to erasure.

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

PART IV

TRANSFER OF PERSONAL DATA OUTSIDE OF GUYANA

23. General principles for transfers.
24. Adequate level of protection.
25. Appropriate safeguards.
26. Binding corporate rules.
27. Transfers of disclosures not authorised by law.
28. Derogations for specific situations.
29. Non-compliance.
30. Substantial public interests.

PART V

EXEMPTIONS

31. Exceptions to the Act.
32. Crime and taxation.
33. Health, education and social work.
34. Regulatory activity.

35. Journalism, literature and art.

36. Research, history and statistics.

37. Certain manual data held by public authorities.

38. Information available to the public by or under law.

39. Disclosures required by law or made in connection with legal proceedings.

40. Parliamentary privilege.

41. Legal professional privilege.

42. Domestic purposes.

43. Confidential references given by the data controller.

44. National security and armed forces.

45. Judicial appointments and honours.

46. Appointments to public service.

47. Corporate finance.

48. Examinations.

49. Refusal to give access to personal data.

50. Powers to make further exemptions by order.

PART VI

DATA CONTROLLER AND DATA PROCESSOR

51. Prohibition on processing without registration.

52. Register of Data Controllers.

53. Notification of changes in respect of a data controller.

54. Responsibility of the data controller.

55. Data protection by design and by default.

56. Joint data controllers.

57. Data processors shall be registered.

58. Register of Data Processors.

59. Notification of changes in respect of a data processor.

60. Data processor.

61. Processing under the authority of the data controller or data processor.

62. Records of processing activities.
63. Cooperation with the Commissioner.
64. Security of processing.
65. Notification of a personal breach to the Commissioner.
66. Communication of a personal breach to the data subject.
67. Data protection impact assessment.
68. Prior consultation.
69. Designation of the data protection officer.
70. Position of the data protection officer.
71. Duties and functions of a data protection officer.

PART VII

DATA PROTECTION COMMISSIONER

72. Establishment of the Data Protection Office.
73. Functions of the Commissioner.
74. Staff.
75. Confidential information.
76. Indemnity.
77. Report.

PART VIII

ENFORCEMENT

78. Enforcement notice.
79. Cancellation of enforcement notice.
80. Request for assessment.
81. Information notice.
82. Special information notice.
83. Determination by Commissioner as to the purposes of journalism or artistic or literary purposes.

84. Restriction on enforcement in case of processing for the purposes of journalism or for artistic or literary purposes.
85. Failure to comply with notice.
86. Service of notice by Commissioner.
87. Warrants.
88. Execution of warrants.
89. Matters exempt from inspection and seizure.
90. Return of warrant.
91. Obstruction of execution of warrant.
92. Aggrieved person may apply to High Court for review.

PART IX

MISCELLANEOUS

93. Data sharing code of practice.
94. Effect of the data sharing code of practice.
95. Certification.
96. International cooperation.
97. Right to compensation and liability.
98. Unlawful obtaining of personal data.
99. Administrative penalty.
100. Liability of body corporate, directors, etc.
101. Prosecutions.
102. Disclosure of information.
103. Access to official documents.
104. Amendment of penalties.
105. Regulations.
106. Review of the Act.

A Bill
Intituled

AN ACT to regulate the collection, keeping, processing, use and dissemination of personal data; to protect the privacy of individuals in relation to their personal data; and provide for related matters.

A.D. 2023 Enacted by the Parliament of Guyana:-

PART I
PRELIMINARY

Short title and commencement.

1. This Act may be cited as the Data Protection Act 2023 and shall come into operation on the day the Minister may, by order, appoint, and different days may be appointed in respect of different provisions of this Act.

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 a natural person, which allow or confirm the unique

identification of that natural person, such as facial images or dactyloscopic data;

"child" means a person who is under the age of eighteen years;

"Commissioner" means the Data Protection Commissioner appointed under section 72;

"consent" means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her and includes any expression of consent given by-

(a) the legal representative of the data subject;

(b) in the case of a person who by reason of a mental illness is unable to act, the nominated representative of the person appointed pursuant to the Mental Health Protection and Promotion Act;

No. 14 of 2022

(c) in the case of a child, the parent or guardian of the child; or

(d) any person to whom the data subject delegates, in writing, the right to give or withhold consent to the processing;

"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) natural or legal person, public authority, agency or other body 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 any law to be processed, the natural or legal person on whom the obligation to process the data is imposed by or under any law;

"data processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"data protection officer" means a person designated as such pursuant to section 69;

"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 a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;

"health care professional" means a person or institution duly licensed under the relevant law to provide health care or health services;

"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;

"identifiable natural person" means a person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the person;

"Minister" means the Minister responsible for data protection;

"prescribed" means prescribed by the Minister by regulations made under the Act;

"personal data" means any information relating to an identified or identifiable natural person;

"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;

"processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and the term "process" shall be construed accordingly;

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects

relating to a natural person, in particular to analyse or predict aspects concerning that natural person'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 are not attributed to an identified or identifiable natural person;

"public authority" means a public office or ministry, department, agency, unit or 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 any law;

"relevant filing system" means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"representative" means the representative of a data controller or data processor who is not established in Guyana and is nominated pursuant to-

(a) section 51(3) in respect of a data controller; or

(b) section 57(3) in respect of a data processor;

"restriction of processing" 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 the data subject, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings;

"third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, is authorised to process personal data.

Scope the 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 Guyana; and

(b) the processing of personal data of data subjects in Guyana by a data controller or a data processor not established in Guyana, where-

(i) the data controller or data processor uses equipment in Guyana for processing the personal data otherwise than for the purpose of transit through Guyana; or

(ii) the processing activities are related to-

(A) the offering of goods or services to data subjects in Guyana;

(B) the monitoring of the behaviour of data subjects as far as their behaviour takes place within Guyana.

(2) For the purposes of subsection (1), "established in Guyana" means-

(a) an individual who is ordinarily resident in Guyana;

(b) a body, association or other entity incorporated, organised, registered, or otherwise formed under any law; or

(c) a person who does not fall within paragraph (a) or (b) but maintains in Guyana-

(i) an office, branch or agency through which the person carries on any activity related to the processing of personal data; or

(ii) a regular practice.

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 the personal data is 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 it is processed, is 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 or she 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 particulars given to the Commissioner pursuant to sections 52 and 53.

(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 shall 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 or her 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) commits an offence and is liable-

(a) on summary conviction to a fine of not less than five million dollars nor more than fifty million dollars or to imprisonment for a term not exceeding two years; or

(b) on conviction on indictment to a fine of not less than twenty million dollars nor more than one hundred million dollars or to imprisonment for a term not exceeding five years.

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 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 law to supply the data; or

(b) required to supply the data pursuant to any Convention or other instrument imposing an international obligation on Guyana.

(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 or her, 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 identity of its data protection officer designated pursuant to section 69;

(iv) the purpose or purposes for which the data is intended to be processed;

(v) the identity of any third party to which disclosure of the personal data is contemplated;

(vi) the legal authority for seeking the personal data, where applicable;

(vii) whether the provision, by the data subject, of the personal data sought is compulsory under any law, and the consequences of not providing the personal data;

(viii) the expected period of retention of the personal data; and

(ix) 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 or her, 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 or her 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 Parliament;

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

(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) 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 of consent.

7. (1) Where processing is based on consent, the data controller shall be able to demonstrate that the data subject has consented to processing of his or her 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) The data subject shall have the right to withdraw his or her consent at any time in respect of the processing of his or her personal data at any time and the data controller shall inform the data subject of his or her right to withdraw prior to him or her giving consent.

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

(5) When assessing whether consent is freely given, utmost account shall be taken of 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 a 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 the principles of contract law under any law concerning 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 or her 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 is not established or conducted for profit and 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 contemplated in subparagraph (i) 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 Parliament;

(j) the processing is necessary for the exercise of any functions conferred on any person by or under a law;

(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 is necessary for reasons of public interests in the areas of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;

(n) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with section 36;

(o) the processing-

(i) is of sensitive personal data consisting of information as to racial or ethnic origin;

(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 that 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 of the National Assembly.

(4) For the purposes of subsection (1)(l), "medical purposes" includes the purposes of preventative or occupational medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health care services.

Processing which does not require identification.

10. (1) Where the purposes for which a data controller processes personal data do not or do not longer require the identification of a data subject by the controller, the data controller shall not be obliged to maintain, acquire, or process additional information in order to identify the data subject for the sole purpose of complying with this Act.

(2) Where, in cases referred to in subsection (1), the data controller is able to demonstrate that he or she is not in a position to identify the data subject, the data controller shall, where possible, inform the data subject as soon as possible.

(3) In the cases set out in subsection (1), sections 11 to 16 shall not apply, except where the data subject, for the purpose of exercising his or her rights under those sections, provides additional information enabling his or her identification.

PART III

RIGHTS OF A DATA SUBJECT

Rights of access.

11. 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; and

(viii) the existence of automated decision-making, including profiling, referred to in section 19 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 25.

(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 in subsection (3) shall not adversely affect the rights and freedoms of other data subjects.

Right to rectification.

12. (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 or her.

(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.

13. (1) The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him or her 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 17 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to section 18;

(d) the personal data has been unlawfully processed; or

(e) the personal data has to be erased in compliance with a legal obligation in Guyana 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 the 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 for-

(a) exercising the right of freedom of expression and information;

(b) compliance with a legal obligation which requires processing by any law to which the data controller is subject or the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

(c) reasons of public interest in the area of public health;

(d) archiving for the purposes of research, history or statistics in accordance with section 36; or

(e) the establishment, exercise or defence of legal claims.

Right to restriction of processing.

14. (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 the data is required by the data subject for the establishment, exercise or defence of legal claims; or

(d) the data subject has objected to processing pursuant to section 17 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 Guyana.

(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 personal data.

15. (1) The data controller shall communicate to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort any-

(a) rectification of personal data pursuant to section 12;

(b) erasure of personal data pursuant to section 13; or

(c) restriction of processing of personal data pursuant to section 14.

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

Right to data portability.

16. (1) The data subject has the right to receive the personal data concerning him or her, which the data subject 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 or her, which he or she 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) The data subject, in exercising his or her right to data portability pursuant to subsections (1) and (2), shall have the right to have his or her

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 the right of erasure.

(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 to receive personal data shall not adversely affect the rights and freedoms of other data subjects.

Right to object.

17. (1) The data subject shall have the right to object in writing at any time to the processing of personal data concerning him or her unless the data controller demonstrates compelling legitimate grounds for the processing which override the data subject's interests, rights and freedoms or for the establishment, exercise or defence of a legal claim.

(2) Where personal data are processed for the purpose of direct marketing, the data subject may object to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

(3) Where a data subject objects to processing of personal data for the purpose of direct marketing, the personal data shall no longer be processed for that purpose.

(4) Where personal data are processed for scientific or historical research purposes pursuant to section 36, the data subject on grounds relating to his or her particular situation, shall have the right to object to processing of

personal data concerning him or her, unless processing is necessary for the performance of a task to be carried out for reasons of public interest.

(5) The rights referred to in subsections (1) and (2) shall be explicitly brought to the attention of the data subject.

(6) In this section, "direct marketing" means the communication of any advertising or marketing material which is directed to any particular individual.

Right to prevent processing likely to cause damage or distress.

18. (1) Subject to subsection (2), a data subject is entitled, in writing, to require the data controller 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 or she 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.

Automated individual decision-making, including profiling.

19. (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 her or similarly significantly affects him or her.

(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 law 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.

20. (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 protection 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 section 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; and

(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 Commissioner, or in the case of transfers to the appropriate safeguards referred to in section 25 and the means by which to obtain a copy of the personal data or where the personal data 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; and

(f) the existence of automated decision-making, including profiling, referred to in section 19 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.

21. (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 protection officer, where applicable;

(c) the purposes of the processing for which the personal data are 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; and

(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 Commissioner, or in the case of transfers to the appropriate safeguards referred to in section 25 and the means to obtain a copy of the personal data or where the personal data 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; and

(g) the existence of automated decision-making, including profiling, referred to in section 19 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 in the public interest, scientific or historical research purposes or statistical

purposes, subject to the conditions and safeguards referred to in section 36 or insofar as the obligation referred to in subsection (1) would likely render impossible or seriously impair the achievement of the objectives of that processing;

(c) obtaining or disclosing the personal data is expressly laid down by any law 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 shall remain confidential subject to an obligation of professional secrecy regulated by any law.

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

22. (1) The data controller shall take appropriate measures to provide any information referred to in sections 20 and 21 and any communication under sections 11 to 19 and section 65 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 or her rights under sections 11 to 16 and section 19 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 11 to 16 and section 19.

(5) The data controller shall provide information on action taken on a request under sections 11 to 16 and section 19 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 11 to 16 and section 19.

(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 or her rights under sections 11 to 16 and section 19 by electronic 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 applying to the High Court for review pursuant to section 92.

(10) Information provided under sections 19 and 20 and any communication and any actions taken under sections 11 to 16, 19 and section 65 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 applying to the High Court for review pursuant to section 92.

(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 11 to 19, 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 sections 20 and 21 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 the icons 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

TRANSFER OF PERSONAL DATA OUTSIDE OF GUYANA

General principles for transfers.

23. Personal data shall not be transferred to a country or territory outside Guyana or an international organisation unless that country, territory or international organisation 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.

24. For the purposes of section 23, 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) the existence and effective functioning of supervisory authorities with responsibility for ensuring and enforcing compliance with data protection laws;

(h) 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

(i) any security measures taken in respect of the data in that country or territory.

Appropriate safeguards.

25. For the purposes of section 23, 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 26;

(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.

26. (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 Guyana;

(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 or Commissioner 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" mean 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 natural or legal person engaged in an economic activity, irrespective of its legal form, including partnerships or associations regularly 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 in a country or territory outside of Guyana.

Transfers or disclosures not authorised by law.

27. Any judgment of a court and any decision of an administrative authority of a country or territory requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement between the requesting country or territory and Guyana, without prejudice to other grounds for transfer pursuant to this Part.

Derogations for specific situations.

28. (1) Sections 23, 24 and 25 shall not apply where-

(a) the data subject has given his or her 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 or her 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 is entered into at the request of the data subject or 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.

(2) Where a transfer could not be based on sections 24, 25 and 26 and none of the derogations for a specific situation referred to in subsection (1) is applicable, a transfer to a country or territory outside of Guyana or an international organisation may take place only if the transfer is not-

(a) repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject; and

(b) the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data to the Commissioner.

(3) Where data is transferred pursuant to subsection (2), the data controller shall inform the Commissioner of the transfer and shall, in addition to providing the information referred to in sections 20 and 21, inform the data subject of the transfer and on the compelling legitimate interests pursued.

(4) A transfer pursuant to subsection (1)(c) shall not involve the entirety of the personal data or entire categories of the personal data contained in the register, where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or in case they are to be the recipients.

(5) Subsection (1)(a) and (b)(i) to (vi) shall not apply to activities carried out by a public authority in the exercise of its functions.

(6) The data controller or data processor shall document the assessment as well as the suitable safeguards referred to in subsection (2)(b) in the records referred to in section 62.

Non-compliance.

29. A person who contravenes section 23, 24 or 25 commits an offence and is liable-

(a) on summary conviction to a fine of not less than ten million dollars nor more than fifty million dollars or to imprisonment for a term not exceeding three years; or

(b) on conviction on indictment to a fine of not less than twenty million dollars nor more than one hundred million dollars or to imprisonment for a term not exceeding five years.

Substantial public interests.

30. (1) The Minister may, by order, specify the-

(a) circumstances in which a transfer of the personal data of data subjects outside of Guyana 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 Guyana, which is not required by or under a law, 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 of the National Assembly.

PART V
EXEMPTIONS

Exceptions to the Act.

31. (1) Except as provided for in this Part, the disclosure to data subject requirements shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information.

(2) In this part-

"disclosure to data subject requirements" means-

(a) the information mentioned in section 5(3) required to be given to a data subject; and

(b) the provisions of section 11;

"the non-disclosure provisions" means the following provisions, to the extent to which the provisions prohibit the disclosure in question-

(a) section 4(1)(a), except to the extent to which it requires compliance with the conditions in sections 6 and 9;

(b) section 4(1) (b), (c), (d), (e); and

(c) sections 12 to 19.

Crime and taxation.

32. (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 sections 6 and 9, and from section 11 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 or her possession for any of the purposes mentioned in subsection (1)(a) to (c),

is exempt from the disclosure to data subject requirements 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) To the extent that an exemption is required in the interests of the operation of a system of risk assessment, personal data is exempt from section 11 where the data controller is a public authority and where that data-

(a) consist of a classification applied to the data subject as a part of the 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 the purposes set out in paragraph (a) (i) and (ii).

Health, education, and social work.

33. (1) The Minister may, by order, exempt from the disclosure to data subject requirements, or modify those requirements 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; or

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

Regulatory activity.

34. (1) Personal data processed for the purposes of discharging any function to which this subsection applies are exempt from the disclosure to data subject requirements to the extent to which the application of those requirements in any case is likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is-

(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;

(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;

(iv) maladministration by public authorities;

(v) failures in services provided by public authorities;

(vi) a failure of a public authority to provide a service which it is a function of the authority to provide; or

(vii) against conduct which may adversely affect their interests by persons carrying on a business;

(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) recovering the property of charities;

(e) securing the health, safety and welfare of persons at work;

(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;

(g) 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

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

(5) For the purposes of subsection (2) "relevant function" means-

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

(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.

35. (1) Personal data which is processed only for the purposes of journalism, or artistic or literary purposes is exempt from the principles of processing personal data 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; or

(c) the data controller reasonably believes that, in all the circumstances, compliance with the principles 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 the data controller's compliance with any code of practice prepared by the Commissioner pursuant to section 93 which is relevant to the publication in question.

(3) 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 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 twenty-four 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 (4) is met.

(4) The conditions referred to in subsection (3) 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.

(5)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.

36. (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 11 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 the data subject's behalf;

(c) at the request, or with the consent, of the data subject or a person acting on the data subject's 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.

Certain manual data held by public authorities.

37. Personal data which falls within paragraph (e) of the definition of "data" in section 2 and is kept in files or sets of files, including their cover

pages, but is not structured according to specific criteria is exempt from Parts II, III, IV and VI.

Information available to the public by or under law.

38. Personal data consisting of information which the data controller is obliged by any law to make available to the public, whether by publishing the information, making it available for inspection, or otherwise and whether gratuitously or on payment of a fee are exempt from-

(a) the disclosure to data subject requirements;

(b) section 4(d) and sections 12 and 15; and

(c) the non-disclosure provisions,

to the extent that the application of paragraphs (a), (b) and (c) would prevent the data controller from complying with the respective obligations.

Disclosures required by law or made in connection with legal proceedings.

39. (1) Personal data is exempt from the non-disclosure provisions where the disclosure is required by any law, rule of law or 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.

40. Where the exemption is required for the purpose of avoiding an infringement of the privileges of Parliament, personal data are exempt from-

(a) Part II, other than the lawfulness requirements set out in section 6; and

(b) Parts III, IV and VI.

Legal professional privilege.

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

Domestic purposes.

42. 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.

43. Personal data is exempt from section 11 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.

National security and armed forces.

44. (1) Personal data is exempt from the disclosure to data subject requirements where the processing of the personal data is required for the purpose of safeguarding national security.

(2) Personal data is exempt from the disclosure to data subject requirements to the extent to which the application of those provisions would be likely to prejudice the combat effectiveness of the armed forces of Guyana.

Judicial appointments and honours.

45. Personal data processed for the purposes of assessing any person's suitability for judicial office or the conferring of any national honour or dignity, is exempt from the disclosure to data subject requirements provisions.

Appointments to public service.

46. The Minister may, by order, exempt from the disclosure to data subject requirements personal data processed for the purposes of assessing any person's suitability for employment in the Public Service, or any office to which appointments are made by the President or by a Minister of Government.

Corporate finance.

47. (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 disclosure to data subject requirements 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 disclosure to data subject requirements 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 Guyana.

(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 disclosure to data subject requirements is required for the purpose of safeguarding an important economic or financial interest of Guyana; 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.

Examinations.

48. Personal data consisting of information recorded by candidates during an academic, professional or other examination and the results from those examination is exempt from section 11.

Refusal to give access to personal data.

49. Where a public authority refuses to give access to personal data, the burden of proof that the information lies within one of the specified exemptions of the Act is on a balance of probabilities and lies upon the public authority.

Powers to make further exemptions by order.

50. (1) The Minister may, by order, exempt from the disclosure to data subject requirements personal data consisting of information the disclosure of which is prohibited or restricted by or under any law where and to the extent that the Minister 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 the Minister 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 of the National Assembly.

PART VI

DATA CONTROLLER AND DATA PROCESSOR

Prohibition on processing without registration.

51. (1) A person shall not operate as a data controller unless he or she 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 that purpose.

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

(4) A person who operates as a data controller without being registered under subsection (1) commits an offence and is liable on summary conviction to a fine of ten million dollars or to imprisonment for two months.

(5) A data controller who is not established in Guyana and who does not nominate a representative pursuant to subsection (3) commits an offence and is liable on summary conviction to a fine of twenty million dollars or to imprisonment for two months.

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

(a) an individual who is ordinarily resident in Guyana;

(b) a body, association or other entity incorporated, organised, registered or otherwise formed under any law; or

(c) any person who does not fall within paragraph (a) or (b) but maintains in Guyana an office, branch, or agency

through which the person carries on any activity related to data processing.

Register of Data Controllers.

52. (1) The Commissioner shall keep a register, to be called the Register of Data Controllers, in which the Commissioner shall cause to be entered in relation to each data controller registered pursuant to section 51, 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 Guyana 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 Guyana within the meaning of section 51(6), the name, address

and other contact information of the representative nominated pursuant to section 51(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.

53. (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 the data controller.

(2) On receiving notification of the data controller under subsection (1) the Commissioner shall make any amendments to the Register of Data Controllers as are necessary.

Responsibility of the data controller.

54. (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.

55. (1) The data controller shall implement appropriate technical and organisational measures which are designed-

(a) to implement the principles set out in section 4 in an effective manner; and

(b) to integrate the necessary safeguards into the processing.

(2) The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing.

(3) The data controller shall implement the appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose is processed, taking into consideration-

(a) the amount of personal data collected;

(b) the extent of its processing;

(c) the period of its storage;

(d) its accessibility; and

(e) the cost of processing data and the technologies and tools used.

(4) To give effect to this section, the data controller shall consider measures such as-

(a) identifying reasonably foreseeable internal and external risks to personal data under the person's possession or control;

(b) establishing and maintaining appropriate safeguards against the identified risks;

(c) the pseudonymisation and encryption of personal data;

(d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) verifying that the safeguards are effectively implemented; and

(f) ensuring that the safeguards are continually updated in response to new risks or deficiencies.

Joint data controllers.

56. (1) Where two or more data controllers jointly determine the purposes and means of processing personal data, they are joint data controllers for the purposes of this Part.

(2) Joint data controllers shall, in a transparent manner, determine their respective responsibilities for compliance with this Part by means of an arrangement between them, except to the extent that those responsibilities are determined under or by virtue of a law.

(3) The arrangement shall designate the data controller that will be the contact point for data subjects.

Data processors shall be registered.

57. (1) A person shall not operate as a data processor unless the person 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 Guyana shall nominate, for the purposes of this Act, a representative established in Guyana.

(4) A person who operates as a data processor without being registered under subsection (1) commits an offence and is liable on summary conviction to a fine of ten million dollars or to imprisonment for two months.

(5) A data processor that is not established in Guyana and who does not nominate a representative pursuant to subsection (3) commits an offence and is liable on summary conviction to a fine of twenty million dollars or to imprisonment for two months.

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

(a) an individual who is ordinarily resident in Guyana;

(b) a body, association or other entity incorporated, organised, registered or otherwise formed under any law; or

(c) any person who does not fall within paragraph (a) or (b) but maintains in Guyana an office, branch, or agency through which he or she carries on any activity related to data processing.

Register of Data Processors.

58. (1) The Commissioner shall keep a register, to be called the Register of Data Processors, in which the Commissioner 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 the data 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 Guyana 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 Guyana within the meaning of section 57(6), the name, address, and other contact information of the representative nominated pursuant to section 57(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.

59. (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 the data processor.

(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.

60. (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; and

(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 Guyana or an international organisation, unless required to do so by any law and in such a case, the data processor shall inform the data controller of that legal requirement before processing, unless the law 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 64;

(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 64 to 68 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 law requires storage of the personal data; and

(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 in 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 a 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.

61. (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 law.

(2) A person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine of ten million dollars or to imprisonment for a term not exceeding three years.

Records of processing activities.

62. (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 protection 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 28, the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data; and

(g) where possible, a general description of the technical and organisational security measures referred to in section 64(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 protection 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 28, the documentation of suitable safeguards; and

(d) where possible, a general description of the technical and organisational security measures referred to in section 64(1).

Cooperation with the Commissioner.

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

Security of processing.

64. (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 or she is required to do so by any law.

Notification of a personal data breach to the Commissioner.

65. (1) Where there is a personal data breach the data controller shall without undue delay and, where feasible, not later than seventy-two 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 any person.

(2) Where the notification of the personal data breach to the Commissioner is not made within seventy-two 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 protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach; and

(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 or her assessment of the data controller's compliance with this section.

Communication of a personal data breach to the data subject.

66. (1) Where a personal data breach is likely to result in a high risk to the rights and freedoms of persons, the data controller shall communicate the

personal data breach to the data subject without undue delay and, where feasible, not later than seventy-two 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 65 (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; and

(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.

(4) Where the data controller has not already communicated the personal data breach to the data subject, the Commissioner may, after having considered the likelihood of the personal data breach resulting in a high risk,

require the data controller to do so or may decide that any of the conditions referred to in subsection (3) are met.

Data protection impact assessment.

67. (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 a person, 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 protection 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 persons that is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning a person or similarly significantly affect the person;

(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 *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 *Gazette*.

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

(a) 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 the Commissioner has prepared data sharing code of conduct pursuant to section 93, compliance with the code by the data controller or data processor shall be taken into consideration when assessing the impact of the processing operations performed by the data controller or the data processor, in particular for the purposes of a data protection impact assessment.

(9) 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.

(10) 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.

68. (1) The data controller shall consult the Commissioner prior to processing where a data protection impact assessment under section 67 indicates that the processing would result in a high risk to the rights and freedoms of any person 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 eight 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 six 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 the Commissioner 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 protection officer;

(e) the data protection impact assessment provided for in section 67; and

(f) any other information requested by the Commissioner.

Designation of the data protection officer.

69. (1) The data controller and the data processor shall designate a data protection 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 protection officer provided that a data protection 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 protection 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 protection officer.

(5)The data protection 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 71.

(6)The data protection 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 protection officer to the Commissioner.

Position of the data protection officer.

70. (1) The data controller and the data processor shall ensure that the data protection 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 protection officer in performing the duties and functions referred to in section 71 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

(3) A data protection officer shall not be dismissed or penalised by the data controller or the data processor for performing duties and functions referred to in section 71.

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

(5) Data subjects may contact the data protection 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 protection officer is required to keep confidential all matters concerning the performance of his or her duties and functions referred to in section 71.

Duties and functions of a data protection officer.

71. (1) A data protection officer shall-

(a) inform and advise the data controller or the data processor and the employees who carry out processing of their obligations under 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 67;

(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 68, and to consult, where appropriate, with regard to any other matter; and

(f) monitor compliance by the controller with this Part.

(2) A data protection officer shall, in the performance of his or her 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

Establishment of the Data Protection Office.

72. (1) There is established for the purposes of this Act, a body corporate be known as the Data Protection Office which shall be responsible for the administration and implementation of this Act.

(2) The President shall appoint a Data Protection Commissioner who shall be a person of eminence in public life with wide knowledge and experience in law, science and technology, management or administration and governance.

(3) The Commissioner shall be the head of the Data Protection Office and shall be responsible for managing the Office and shall discharge the functions assigned to him or her under this Act.

(4) The President may remove the Commissioner from office if the Commissioner-

(a) is adjudged as insolvent;

(b) has been convicted of an offence which involves moral turpitude;

(c) is unfit to continue in office by reason of any illness; or

(d) had, or has, acquired such financial or other interest as is likely to affect prejudicially his or her functions as Commissioner.

(5) Before removing the Commissioner from office, the President shall afford the Commissioner an opportunity to be heard.

Functions of the Commissioner.

73. In addition to any other 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 or her 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;

(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 or her 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 Guyana, 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) where appropriate, monitor the implementation of codes of practice prepared pursuant to section 93;

(s) where applicable, carry out periodic review of certifications issued pursuant to section 95;

(t) recommend the adoption and development of standard contractual clauses and standard data protection clauses pursuant to this Act;

(u) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to section 67(5) and (6);

(v) investigate complaints from persons concerning abuses in the processing of personal data;

(w) approve binding corporate rules pursuant to section 26;

(x) keep internal records of contraventions of this Act and of measures taken to address those contraventions; and

(y) exercise such other functions as are conferred or imposed on the Commissioner by or under this Act or any other law.

Staff.

74. (1) The Minister shall provide the Data Protection Office with such officers and employees as may be necessary for the efficient discharge of the Commissioner's functions under this Act.

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

Confidential information.

75. (1) The Commissioner and any person appointed pursuant to section 74(1) shall keep secret all confidential information coming to his or her knowledge during the course of the administration of this Act, 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 law; or

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

(3)Subject to subsection (2), any person who contravenes subsection (1) commits an offence and is liable on summary conviction to a fine not exceeding ten million dollars or to imprisonment for a term not exceeding six months.

(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 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.

76. The Commissioner and the staff of the Data Protection Office 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 any staff of the Office pursuant to this Act.

Report.

77. (1) The Commissioner shall, not later than three months after the end of each financial year, submit to the Minister a report of the activities and operations of the Office 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 laid in the National Assembly not later than three months from the date of receipt thereof by the Minister.

PART VIII

ENFORCEMENT

Enforcement notice.

78. (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 the data controller or data processor an enforcement notice requiring the data controller or data processor, to-

(a) take within such time as may be specified in the notice, or to refrain from taking after such time as may be so specified, such steps as are so specified; or

(b) refrain from processing any personal data, or any personal data of a description specified in the notice, or to refrain from processing 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 has been or is being contravened and the reasons for reaching that conclusion; and

(b) particulars of the right of review conferred by section 92.

(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 a review can be sought against the notice pursuant to section 92 and, where a review is sought, the notice need not be complied with pending the determination or withdrawal of the application for review.

(5) Where, by reason of special circumstances, the Commissioner considers that an enforcement notice should be complied with as a matter of

urgency the Commissioner may include in the notice a statement to that effect and a statement of the Commissioner's 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 seven days beginning with the day on which the notice is served.

Cancellation of enforcement notice.

79. (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, the Commissioner 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 a review can be sought pursuant to section 92 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.

80. (1) A request may be made to the Commissioner by or on behalf of any person who is, or believes himself or herself 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 the Commissioner to be appropriate, unless he or she is not supplied with such information as he or she may reasonably require to-

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

(b) enable him or her 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 or her 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 11.

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

(a) whether the Commissioner has made an assessment as a result of the request; and

(b) to the extent that the Commissioner considers appropriate, having regard in particular to any exemption from section 11 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request.

Information notice.

81. (1) The Commissioner may serve the data controller with an information notice requiring the data controller to furnish the Commissioner

with the required information relating to the request or to compliance with the provisions of this Act, where the Commissioner-

(a) has received a request under section 80 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.

(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 80 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 the Commissioner's reasons for regarding it as relevant for that purpose; and

(b) particulars of the right of review conferred by section 92.

(3) The Commissioner may specify in an information notice-

(a) the form in which the information shall be furnished; and

(b) the period within which, or the time and place at which, the information shall be furnished.

(4) Subject to subsection (5), a period specified in an information notice under subsection (3)(b) shall not end, and a time so specified shall not fall, before the end of the period within which a review can be applied for pursuant to section 92 against the notice and, where a review is sought, the information need not be furnished pending the determination or withdrawal of the application for review.

(5) Where by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, the Commissioner may include in the notice a statement to that effect and a statement of the Commissioner's 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 seven 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 an attorney-at-law and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights under this Act; or

(b) any communication between an attorney-at-law and his or her client, or between such an adviser or his or her 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 High Court, and for the purposes of such proceedings.

(7) 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.

(8) Any relevant statement, whether oral or written, 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 85, unless in the proceedings-

(c) in giving evidence the person provides information that is inconsistent with it; and

(d) evidence relating to it is adduced, or a question relating to it is asked, by that person or on that person's behalf.

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

(10) This section has effect subject to section 84(3).

Special information notice.

82. (1) The Commissioner may serve the data controller with a special information notice, requiring the data controller to furnish the Commissioner with specified information for the purpose specified in subsection (2), where the Commissioner-

(a) receives a request under section 80 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 35, 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.

(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 shall contain-

(a) particulars of the right of review conferred by section 92; and

(b) in a case falling within-

(i) subsection (1)(a), a statement that the Commissioner has received a request under section 80 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 shall be furnished; and

(b) the period within which, or the time and place at which, the information shall be furnished.

(5) Subject to subsection (6), a period specified in a special information notice under subsection (4)(b) shall not end, and a time so specified shall not fall, before the end of the period within which a review can be applied for pursuant to section 92 against the notice and, where a review is sought, the information need not be furnished pending the determination or withdrawal of the application for review.

(6) Where by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, the Commissioner may include in the notice a statement to that effect and a statement of his or her 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 seven 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 an attorney-at-law and his or her 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 an attorney-at-law and his or her client, or between such an adviser or his or her 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 High Court, and for the purposes of such proceedings.

(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 the 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 any offence under this Act, other than an offence under section 85, 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.

(10) 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.

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

(12) 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.

83. (1) The Commissioner may make a determination in writing 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.

(2) Notice of the determination shall be given to the data controller and the notice shall contain particulars of the right of review conferred by section 92.

(3)A determination under subsection (1) shall not take effect until the end of the period within which a review can be sought pursuant to section 92 and, where a review is sought, shall not take effect pending the determination or withdrawal of the application for review.

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

84. (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 83 (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 the High Court 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 83 (1) with respect to those data has taken effect.

Failure to comply with notice.

85. (1) A person who fails to comply with an enforcement notice, an information notice or a special information notice commits an offence and is liable on summary conviction to a fine of one million dollars or to imprisonment for three months.

(2) A person who, in purported compliance with an information notice makes a statement which the person knows to be false in a material respect or recklessly makes a statement which is false in a material respect, commits an offence and is liable on summary conviction to a fine of one million dollars or to imprisonment for three months.

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

Service of notice by Commissioner.

86. (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) a natural person, be served on the person by-

(i) delivering it to the person;

(ii) sending it to the person by post addressed to the person at the person's usual or last known place of residence or business; or

(iii) leaving it for the person 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 body corporate 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.

87. (1) A judge of the High Court may issue a warrant where that judge 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.

(2) A warrant issued under subsection (1) shall authorise a police officer accompanied by the Commissioner, staff or any other person skilled in information technology as the police officer may deem necessary for the purpose, within seven 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; and

(e) require any person on the premises to provide-

(i) an explanation of any document or other material found on the premises; or

(ii) any 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 83 with respect to those data has taken effect.

Execution of warrants.

88. (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, the person 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.

89. (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 44(1), 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) an attorney-at-law and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights under this Act; or

(b) an attorney-at-law and his or her client, or between such an adviser or his or her 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 High Court and for the purposes of those proceedings.

Return of warrant.

90. A warrant shall be returned to the High Court after being executed or 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 that police officer under the warrant.

Obstruction of execution of a warrant.

91. 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 the warrant such assistance as the police officer may reasonably require for the execution of the warrant;

(c) makes a statement in response to a requirement under section 87(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 87(2)(e) which is false in a material respect,

commits an offence and is liable on summary conviction to a fine of one million dollars or to imprisonment for six months.

Aggrieved person may apply to High Court for review.

Cap. 3:06

92. Any person aggrieved by a decision of the Commissioner under this Act may apply to the High Court for judicial review in accordance with the Judicial Review Act.

PART IX
MISCELLANEOUS

Data sharing code of practice.

93. (1) The Commissioner may prepare and submit to the Minister a data sharing code of practice which contains-

(a) practical guidance in relation to the sharing of personal data in accordance with the requirements of this Act; and

(b) such other guidance as the Commissioner considers appropriate to promote good practice in the sharing of personal data.

(2) Before a data sharing code of practice is prepared under this section, the Commissioner shall consult any of the following as the Commissioner considers appropriate-

(a) trade associations;

(b) persons who appear to the Commissioner to represent the interests of data controllers;

(c) data subjects; and

(d) persons who appear to the Commissioner to represent the interests of data subjects.

(3) In this section, a reference to the sharing of personal data is to the disclosure of the personal data by transmission, dissemination or otherwise making the data available.

(4) Where a data sharing code of practice is submitted to the Minister under subsection (1), the Minister shall-

(a) approve the code; or

(b) withhold approval of the code if it appears to the Minister that the terms of the code could result in Guyana being in breach of any of its international obligations and shall promptly inform the Commissioner of the reasons for withholding approval.

(5) Where a data sharing code of practice is not approved under subsection (4)(b), the Commissioner shall prepare another code of practice in accordance with this section.

(6) A data sharing code of practice which is approved under subsection (4)(a) comes into operation upon the publication of the code in the *Gazette*, unless a later date is specified in the code as the date on which it is to come into operation, in which case the code shall come into operation on that later date.

(7) The Commissioner shall keep the data sharing code of practice under review and in any event shall review the code within eighteen months after the code first comes into operation and thereafter at least once every three years.

(8) Any amendment or repeal of the data sharing code of practice shall be done in accordance with the procedure set out in this section for the making of the code, including the provisions as to prior consultation.

Effect of data sharing code of practice.

94. (1) A failure on the part of any person to act in accordance with any provision of the data sharing code of practice does not of itself render that person liable to any legal proceedings in any court.

(2) The data sharing code of practice is admissible in evidence in any legal proceedings.

(3) If any provision of the data sharing code of practice appears to-

(a) a court conducting any proceedings under this Act;

(b) a court conducting any other legal proceedings; or

(c) the Commissioner carrying out any function under this Act,

to be relevant to any question arising in the proceedings, or in connection with the exercise of that jurisdiction or the carrying out of those functions, in relation to any time when the code was in force, that provision of the code shall be taken into account in determining that question.

Certification.

95. (1) The Commissioner may, in order to encourage compliance of processing operations by data controllers and data processors with this Act, lay down technical standards for data protection certification mechanisms and data protection seals and marks.

(2) A certification shall be –

(a) voluntary;

(b) issued to a data controller or data processor for a maximum period of three years and may be renewed under the same conditions where the relevant requirements continue to be met; and

(c) withdrawn where the requirements for the certification are no longer met.

(3) Where a data controller or data processor seeks certification under this section, he or she shall provide to the Commissioner all information and access to his or her or its processing activities which are necessary to conduct the certification procedure.

(4) A certification issued under this section shall not alter the responsibility of the data controller or data processor for compliance with this Act.

International cooperation.

96. The Minister may, after consultation with the Minister responsible for foreign affairs, make regulations as to co-operation by the Commissioner with authorities in foreign States exercising functions analogous to those of the Commissioner under this Act, in connection with the performance of their respective duties and, in particular, as to the exchange of information with such authorities.

Right to compensation and liability.

97. (1) Any person 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 a person pursuant to subsection (1), it is a defence for the data controller or the data processor to prove that he or she 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.

98. (1) Subject to subsection (2), 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 law, by any rule of law or by the order of a court of competent jurisdiction;

(b) the person acted in the reasonable belief that he or she 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) the person acted in the reasonable belief that he or she 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) commits an offence.

(4) A person who sells personal data commits an offence if he or she obtained the data in contravention of subsection (1).

(5) A person who offers to sell personal data commits an offence where the person-

(a) obtains the personal data in contravention of subsection (1); or

(b) subsequently obtains the personal data in contravention of subsection (1).

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

(7) For the purposes of subsections (4) to (6), "personal data" includes information extracted from personal data.

(8) A person who commits an offence under this section is liable-

(a) on summary conviction to a fine of not less than twenty million dollars nor more than one hundred million dollars or to a term of imprisonment not exceeding five years; or

(b) on conviction on indictment to a fine of not less than twenty million dollars nor more than five hundred million dollars or to a term of imprisonment not exceeding ten years.

Administrative penalty.

99. (1) Where the Commissioner after a hearing determines that a person has contravened sections 53(1), 59(1) and sections 62 to 69 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 State an administrative penalty of an amount not exceeding ten million dollars.

(2) In addition to the public interest, where the Commissioner seeks to make an order pursuant to subsection (1), the Commissioner 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;

(h) compliance by the data controller or data processor with any order of the Commissioner;

(i) adherence to any data sharing code of practice or approved certification mechanisms; and

(j) 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 a review has been filed pursuant to section 92.

(4) A penalty imposed by the Commissioner in the exercise of the Commissioner's powers under this Act shall be payable into the Consolidated Fund and may be recovered by the State 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.

Liability of body corporate, directors, etc.

100. (1) Notwithstanding any other penalty specified in this Act, where a body corporate commits an offence under this Act, the body corporate shall be liable to a fine not exceeding four percent of the annual gross worldwide turnover of that body corporate for the preceding financial year.

(2) In determining the quantum of any fine under subsection (1), a court shall take into account-

(a) the estimated economic cost to consumers, users of the services concerned and any other persons, of the contravention giving rise to the offence;
(b) the estimated economic benefit derived by the body corporate from the commission of the offence;
(c) the period for which the contravention continued;
(d) the number and severity of any other offences under this Act committed by the body corporate; and
(e) any other factors which the court considers relevant.

(3) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary, similar officer of the body corporate or any person who was purporting to act in any such capacity, that director, manager, secretary, similar

officer or other person, as the case may be, shall be liable, as well as the body corporate to be proceeded against and punished accordingly.

(4) Where the affairs of a body corporate are managed by its members, subsection (3) shall apply in relation to the acts and defaults of a member in connection with that member's functions of management as if the member was a director of the body corporate.

Prosecutions.

101. (1) No proceedings for an offence under this Act shall be instituted except-

(a) by the Director of Public Prosecutions; or

(b) by the Commissioner, with the consent of the Director of Public Prosecutions.

(2) The court by or before which the person is convicted may order a document or other material to be forfeited, destroyed or erased if-

(a) it has been used in connection with the processing of personal data; and

(b) it appears to the court to be connected with the commission of the offence, subject to subsection (3).

(3) Where a person, other than the offender, who claims to be the owner of the material, or to be otherwise interested in the material, applies to be heard by the court, the court shall not make an order under subsection (2) without giving the person an opportunity to show why the order should not be made.

(4) Subsections (2) and (3) apply where a person is convicted of an offence under section 51, section 85 or section 98.

Disclosure of information.

102. No law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Commissioner or the High Court with any information necessary for the discharge of their functions under this Act.

Access to official documents.

103. (1) For the avoidance of doubt, personal data in any official document held by a public authority or private entity for the performance of a task to be carried out in the public interests may be disclosed by that authority or entity in accordance with any law to which that public authority or private entity may be subject.

(2) In this section "official document" means any document held by a public authority or private entity in connection with its functions and for the purposes of this definition a public document is held by a public authority or private entity if it is in its possession, custody or power.

Amendment of penalties.

104. The Minister may, by order, amend the penalties set out in this Act.

Regulations.

105. (1) The Minister may make regulations for the purpose of giving effect to the provisions of this Act.

(2) Without limiting the generality of subsection (1), regulations made under this section may-

(a) provide for additional safeguards in relation to sensitive personal data, including the processing of national identification numbers, national health identification numbers or any other identifier of general application;

(b) provide for processing of employee's personal data;

(c) provide for the obligation of professional secrecy;

(d) prescribe retention periods for personal data to be observed by data controllers;

(e) prescribe fees which may be imposed under this Act;

(f) prescribe offences for the contravention of the regulations and the penalties therefor, which penalties may not exceed twenty million dollars; and

(g) prescribe the methods by which personal data may be disposed.

Review of the Act.

106. This Act shall be reviewed every five years from the earliest day appointed under section 1.

EXPLANATORY MEMORANDUM

The purpose of this Bill is to protect a person's right to protection with respect to the processing of personal data. Personal data is defined as any information relating to an identified or identifiable natural person. This includes data pertaining to the private life of a person, which includes professional activities, as well as information concerning the person's public life.

This Bill also recognises a person's right to privacy which is universally recognised as one of the inalienable rights of humans. As noted in Article 12 of the Universal Declaration of Human Rights, 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence'. Similarly, Article 17 of the International Covenant on Civil and Political Rights recognises the right to privacy.

The right to respect private life and the right to protection of personal data are interlinked. Both are essential for the fulfilment of other rights such as the freedom of expression, freedom of peaceful assembly and association, and freedom of religion.

Moreover, due to the development in the field of information, communication and technology and the rise in cybercrimes the need to protect personal information is all the more important.

It is important to note that the rights captured in this Bill are not absolute but may be limited if necessary for protecting the rights and freedoms of others. In fact, the very act of processing of personal data is considered lawful interference with rights and freedoms. For this reason, the Bill sets out the legal parameters within which data can be processed in accordance with law.

Consequently, the objects of the Bill are to-

(a) define the general principles of data protection and the rights of data subjects;
(b) protect personal data collected, used or stored by both private and public entities; and
(c) provide for enforcement mechanisms, including penalties, for failure to process personal data in accordance with the law.

PART I of the Bill, which includes clauses 1 to 3, sets out the short title and commencement of the Act, the definition of key words and terms used in the Bill and the scope of the Act. Importantly, the Minister is empowered to assign different days for different provisions of the

Act to come into operation. As it relates to the application of the Act, **clause 3 of the Bill** indicates that this law shall be applicable to the processing of personal data by data controllers and data processors-

(a) who are established in Guyana; or

(b) who, although not established in Guyana-

i. uses equipment located in Guyana for the processing of personal data (otherwise than for transit through Guyana); or

ii. processes personal data of an individual in Guyana, and the processing activities are: –

A. related to the offering of goods or services to individuals in Guyana, regardless of whether a fee is required; or

B. related to the monitoring of the behaviour of individuals insofar as their behaviour takes place within Guyana.

The clause also defines "established in Guyana" as including residency or incorporation under the laws of Guyana and requires a data controller established outside of Guyana to appoint a representative established in Guyana.

PART II of the Bill, which includes clauses 4 to 10, sets out the data protection principles. These principles are that personal data must be-

(a) processed lawfully, fairly, and in a transparent manner;

(b) collected for specified, explicit, and legitimate purposes only;

(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;

(e) kept in a form which permits identification of data subjects for no longer than is necessary; and

(f) processed in a manner that ensures appropriate security of the personal data.

This Part further provides for the general principles governing the conditions of consent in relation to the processing of personal data. Consent must be freely given, informed, specific, and unambiguous and be in the form of a statement or clear affirmative action signifying agreement to the processing. The data subject has the right to withdraw their consent at any time. Data controllers have the duty to keep a verifiable record of the consent. As it relates to a child, 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.

Concerning the processing of sensitive personal data, this Part sets out that the processing of sensitive personal data is prohibited in principle. Sensitive personal data means personal data consisting of information on a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of a political body or trade union, genetic and biometric data, financial or criminal record, a person's sex life or sexual orientation. There is, however, an exhaustive list of exemptions to this prohibition, which can be found in **clause 9 of the Bill** and which amount to lawful grounds for processing sensitive personal data. These exemptions include situations where the data subject explicitly consents to the data processing, processing concerns data explicitly made public by the data subject, processing is necessary to establish, exercise or defend legal claims or when courts act in their judicial capacity or for preventative or occupational medicine purposes.

PART III of the Bill, which includes clauses 11 to 22, provides for the rights of the data subject. Every data subject has the right to information about any data controller's processing of his or her personal data, subject to limited exemptions. Data subjects shall have the right to-

(a) access their own data and obtain certain information about the processing;
(b) have their data rectified by the controller processing their data, if the data are inaccurate;
(c) have the data controller erase their data, as appropriate, if the data controller is processing their data illegally;
(d) temporarily restrict processing;
(e) have their data ported to another data controller under certain conditions;
(f) object to processing on grounds relating to their particular situation and the use of their data for direct marketing purposes.

Additionally, data subjects have the right not to be subject to decision-making based solely on automated processing, including profiling, that have legal effects or that significantly affect him or her. This means that data subjects have the right to obtain human intervention on the part of the data controller and express their point of view and contest a decision based on automated processing.

Further, this Part sets out the information which must be provided to the data subject by the data controller where personal data is collected from the data subject as well as where personal data was not obtained from the data subject. Moreover, this Part makes provision for general principles governing transparent information, communication and modalities for the exercise of the rights of the data subject.

PART IV of the Bill makes provision for general principles governing the appropriate safeguards which must be in place where there is a transfer of the personal data of data subjects outside of Guyana. The free flow of data for the purposes of international trade and cooperation is important, however, the transfer of data outside of Guyana enhances the risk of personal data being misused. Accordingly, this Part provides that personal data shall not be transferred to a state or territory outside of Guyana unless that state or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The adequacy of the protection is determined by a list of factors which includes-

(a) the nature of the personal data;
(b) the state or territory of origin or final destination of the personal data;
(c) the purposes for which and the period during which the personal data are intended to be processed;
(d) the law in force in the state or territory in question; and
(e) the security measures taken in relation to personal data in the destination state or territory.

It should be noted that there are exceptions to this standard. The exceptions include where the data subject consents to the transfer, where the transfer is necessary for reasons of substantial public interest, and where the transfer is for the purposes of national security or the prevention,

detection or investigation of crime. Moreover, this Part provides that data controllers and data processors shall develop binding corporate rules which will govern the transfer of the personal data outside of Guyana. Binding corporate rules mean personal data protection policies which are adhered to by a data controller or data processor for transfers of personal data to a data controller or a data processor outside of Guyana within a group of undertakings, or group of enterprises engaged in a joint economic activity.

Any person who fails to comply with the provisions of this Part commits an offence and is liable to a fine of up to one hundred million dollars and to imprisonment for five years.

PART V of the Bill, which comprises clauses 31 to 50, sets out the instances in which a data controller will not be required to comply with certain provisions of the legislation. Personal data processed for the prevention, detection or investigation of crime, the apprehension or prosecution of offenders, the assessment or collection of any tax or duty, are exempted from the principle that data shall be processed fairly and lawfully, the provisions regarding the right of access to personal data and the non-disclosure provisions. The non-disclosure provisions are those provisions which prohibit the disclosure of personal data.

Personal data which are processed only for special purposes (that is, journalism, artistic or literary purposes) are exempt from the data protection principles. However, exemption is only permissible where-

(a) the processing is with a view to publishing any journalistic, literary or artistic material;
(b) the publication would be in the public interest; and
(c) in all the circumstances, compliance with the principles would be incompatible with the special purposes.

Personal data which are processed only for research purposes (which includes statistical and historical purposes) are exempt where the data are not processed to support measures or decisions regarding particular individuals and the data are not processed in such a way that substantial distress is, or is likely to be, caused to any data subject.

Some other exemptions include-

(a) personal data kept manually but are not structured;

(b) personal data consisting of information which the data controller is obliged under any law to make available to the public;

(c) personal data which is required to be disclosed under any law or order of a court;

(d) personal data that falls within parliamentary privilege and legal professional privilege;

(e) personal data processed for domestic purposes;

(f) personal data consisting of a reference or given in confidence for the purposes of education, employment etc;

(g) personal data processed for the purpose of national security and effectiveness of the armed forces;

(h) personal data processed for corporate finance services; and

(i) personal data processed for the purposes of judicial appointment.

In addition to the exemptions provided for in this Part, the Minister may, by order, make other exemptions as necessary.

PART VI of the Bill, comprising clauses 51 to 71, sets out the obligations of the data controller, data processor and data protection officer. A data controller is any 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 where personal data is processed only for the purpose for which the data is required by or under any law to be processed, the person on whom the obligation to process the data is imposed by or under any law. Under the Act, data controllers must be registered, and where the data controller is not established in Guyana, the data controller must nominate a representative established in Guyana.

It is a criminal offence for a data controller to operate without being registered or without nominating a representative. A person who operates as a data controller without being registered is liable on summary conviction to a fine of ten million dollars or to imprisonment for two months. A data controller who is not established in Guyana and who does not nominate a representative is liable on summary conviction to a fine of twenty million dollars or to imprisonment for two months.

The responsibilities of a data controller include implementing the appropriate technical and organisational measures to ensure that processing is performed according to the law. The data

controller is also mandated to conduct a data protection impact assessment where the type of processing is likely to result in a high risk to the rights and freedoms of a person. The data controller shall consult the Commissioner prior to processing data where a data protection impact assessment indicates that the processing would result in a high risk to the rights and freedoms of any person in the absence of measures taken by the data controller to mitigate the risk.

Like data controllers, data processors must also be registered, and when necessary appoint a representative established in Guyana. A data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller. Processing by a data processor shall be governed by a written contract between the data processor and the data controller. Moreover, the data processor and any person acting under the authority of the data controller or the data processor, who has access to personal data shall not process those data except on instructions from the data controller. It is a criminal offence for a data processor to operate without being registered or without nominating a representative or to process data without lawful authority.

Both a data controller and a data processor shall-

(a) maintain a record of processing activities;
(b) cooperate with the Commissioner;
(c) implement appropriate technical and organisational measures to ensure a level of security when processing data;
(d) notify the Commissioner and the data subject when there is a breach of personal data.

The data controller and the data processor shall designate a data protection officer where the processing is carried out by a public authority, the core activities of the data controller or data processor consists of processing operations which require regular and systematic monitoring of data subjects on a large scale, or the core activities of the data controller or data processor consists of processing on a large scale of sensitive personal data. The duties and functions of a data protection officer include-

(a) informing and advising the data controller or data processor and the employees who carry out processing of their obligations under Act;

(b) monitoring compliance with the Act;

(c) provide advice on data protection impact assessments;

(d) cooperating with the Commissioner; and

(e) acting as the contact person for the Commissioner on issues relating to processing.

PART VII of the Bill, which includes clauses 72 to 77, establishes the Data Protection Office and sets out the functions of the Commissioner. The Data Protection Office is established as a body corporate and shall be responsible for the administration and implementation of the Act. The Commissioner is appointed by the President. Some of the functions of the Commissioner are to-

(a) monitor and enforce the application of the Act;

(b) promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing;

(c) organise activities addressed specifically to children to educate them about the risks, rules, safeguards and rights in relation to processing;

(d) conduct 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 the Act;

(e) maintain a register of data controllers and data processors;

(f) investigate complaints from persons concerning abuses in the processing of personal data.

The Minister shall provide the Data Protection Office with the necessary staff. The Commissioner and staff of the Office shall keep secret all confidential information coming to their knowledge during the course of administering the Act. This Part also provides for the protection of the Commissioner and the staff from legal proceedings where they have carried out their functions under this Act in good faith. Additionally, this Part imposes an obligation on the Commissioner to prepare a report on the Office's activities under the Act for presentation to the Minister and subsequently to National Assembly.

PART VIII of the Bill, which includes clauses 78 to 92, sets out the enforcement powers of the Commissioner. This Part empowers the Commissioner to issue enforcement notices in instances where the Commissioner is satisfied that a data controller has contravened, or is contravening, any of the data protection standards. The Commissioner must consider whether the contravention has caused or is likely to cause any individual damage or distress at the point when deciding to serve an enforcement notice. The notice issued may require the data controller to-

(a) take or refrain from taking specific steps within a specified time;
(b) refrain from processing any personal data or personal data of a specified description; or
(c) refrain from processing data for a specific purpose or in a specific manner, after a specified time.

Compliance with an enforcement notice is not required until the expiration of the period within which a review is sought. If there is an application for review, the notice need not be complied with pending the determination or withdrawal of the review application. Notwithstanding, compliance with the notice will be required if the Commissioner includes a statement to the effect that by reason of special circumstances the enforcement notice should be complied with and specifies a time, no less than seven days, within which compliance is required.

This Part provides that any person who is, or believes himself or herself to be, directly affected by any processing of personal data, to require the Commissioner to carry out an assessment of whether the legislation is being complied with. When the Commissioner receives a request, the Commissioner shall make an assessment and may serve the data controller with an information notice requiring the data controller to furnish the Commissioner with the required information relating to the request or to comply with the provisions of the Act. It is to be noted that a person cannot be required to furnish the Commissioner with any information that is subject to legal professional privilege or that would expose him or her to proceedings for an offence by revealing evidence of the commission of that offence.

The Commissioner under this Part is also empowered to serve the data controller with a special information notice to ascertain whether personal data is being processed only for the purposes of journalism or for artistic or literary purposes, or with a view to the publication of any

journalistic, literary or artistic material. No one is required to furnish the Commissioner with any information where the furnishing would reveal evidence of the commission of an offence or expose the person to proceedings for that offence.

Failure to comply with an enforcement notice, an information notice or a special information notice is an offence which carries a penalty of a fine of one million dollars or imprisonment for three months.

This Part also provides for the issuance of a warrant by a judge of the High Court to authorise a police officer accompanied by the Commissioner, staff or any other person skilled in information technology to, *inter alia*, enter any premises, search the premises, inspect, examine and seize any document or other material found on the premises. A judge shall not issue a warrant in respect of any personal data processed for the purpose of journalism or for artistic or literary purposes unless the Commissioner has determined that the data is not being processed only for that purpose. The powers of inspection and seizure shall not be exercisable in respect of any communication between an Attorney-at-law and their client.

It is an offence for any person to obstruct the execution of a warrant and the penalty for this offence is a fine of one million dollars or imprisonment for six months. Any person aggrieved by a decision of the Commissioner under this Act may apply to the High Court for judicial review in accordance with the Judicial Review Act, Cap. 3:06.

PART IX of the Bill, which includes clauses 93 to106, contains the general provisions of the Bill and provisions relating to penalties. This Part states that the Commissioner may prepare data sharing code of practice which shall be submitted for approval of the Minister. Additionally, the Commissioner may lay down technical standards for data protection certification mechanisms and data protection seals and marks in order to encourage compliance of processing operations by data controllers and data processors.

This Part also provides that the Minister, in consultation with the Minister of Foreign Affairs, may make regulations to facilitate co-operation between the Commissioner and other authorities in foreign States exercising functions analogous to those of the Commissioner.

This Part further provides that any person who suffers damage or distress due to any contravention of the Act by the data controller or data processor is entitled to compensation from that controller or processor.

This Part also sets out that it is an offence to knowingly or recklessly, without the consent of the data controller, obtain or disclose personal data or the information contained in personal data, or procure the disclosure to another person of the information contained in personal data. This offence will not be held to have been committed if the person is able to show, *inter alia*, that the obtaining, disclosing or procuring was required or authorised by or under any law, by any rule of law, or by a court order, or was justified in the public interest. Additionally, it is an offence to sell personal data which was obtained or procured without the data controller's consent. Also, it is an offence for a person to offer to sell, by advertisement or otherwise, personal data which was obtained or procured without the data controller's consent.

The penalties for the above-mentioned offences are a fine of not less than twenty million dollars nor more than one hundred million dollars or a term of imprisonment not exceeding five years (on summary conviction) and a fine of not less than twenty million dollars nor more than five hundred million dollars or a term of imprisonment not exceeding ten years (conviction on indictment).

Further, under this Part the Commissioner is empowered to impose an administrative penalty not exceeding ten million dollars.

Where an offence is committed by a body corporate, the directors, managers, secretaries and other similar officers of that body corporate may be held liable. Additionally, the body corporate may be liable to a fine not exceeding 4% of its annual gross worldwide turnover for the preceding year of assessment.

This Part also provides that the Commissioner may institute proceedings with the consent of the Director of Public Prosecutions.

Further, this Part provides that no law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Commissioner or the High Court with any information necessary for the discharge of their functions under this Act. Moreover, personal

data in any official document held by a public authority or private entity for the performance of a task to be carried out in the public interests may be disclosed by that authority or entity in accordance with any law to which that public authority or private entity may be subject.

Finally, this Part empowers the Minister to amend, by order, the penalties in the Act and gives the Minister the power to make regulations for the purpose of giving effect to the provisions of the Act.

Hon. Brigadier Mark Phillips, M.P.
Prime Minister