

**BELIZE:**

**DATA PROTECTION BILL, 2021**

**ARRANGEMENT OF CLAUSES**

**PART I**

*Preliminary*

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

**PART II**

*Data Protection Principles*

4. Principles relating to processing of personal data.
5. Duty of data controller to comply with principles.
6. Fairness of processing.
7. Lawfulness of processing.
8. Conditions for consent.
9. Conditions applicable to child's consent.
10. Processing of sensitive personal data.

**PART III**

*Rights of a Data Subject*

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

## *Data Protection*

---

14. Right to restriction of processing.
15. Notification regarding rectification or erasure of personal data or restriction of processing of personal data.
16. Right to data portability.
17. Right to prevent processing likely to cause damage or distress.
18. Right to prevent processing for purposes of direct marketing.
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 the rights of the data subject.

## PART IV

### *Transfers of Personal Data outside of Belize*

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

## PART V

### *Exemptions*

30. References to subject information provisions and non-disclosure provisions.
31. National Security.
32. Crime and taxation.
33. Health, education and social work.
34. Regulatory activity.
35. Journalism, literature and art.
36. Research, history and statistics.
37. Manual data held by public authorities.
38. Information available to the public by or under enactment.
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. Armed forces.
45. Judicial appointments and honours.
46. Appointments to public service.
47. Corporate finance.
48. Negotiations with data subject.
49. Examinations.
50. Powers to make further exemptions by order.

## *Data Protection*

---

### *Data Sharing*

- 51. Agencies to share information.
- 52. Relationship between this Part and other law relating to data disclosure.

## PART VII

### *Data Controller and Data Processor*

- 53. Compliance.
- 54. Responsibility of the data controller.
- 55. Data protection by design and by default.
- 56. Data processor.
- 57. Processing under the authority of the data controller or data processor.
- 58. Records of processing activities.
- 59. Cooperation with the Commissioner.
- 60. Security of processing.
- 61. Notification of a personal data breach to the Commissioner.
- 62. Communication of a personal data breach to the data subject.
- 63. Data protection impact assessment.
- 64. Prior consultation.
- 65. Designation of the data privacy officer.
- 66. Position of the data privacy officer.
- 67. Duties and functions of a data privacy officer.

PART VIII

*Data Protection Commissioner*

- 68. Data Protection Commissioner.
- 69. Functions of Commissioner.
- 70. Staff.
- 71. Confidential information.
- 72. Indemnity.
- 73. Report.

PART IX

*Enforcement*

- 74. Enforcement notice.
- 75. Cancellation of enforcement notice.
- 76. Request for assessment.
- 77. Information notice.
- 78. Special information notice.
- 79. Determination by Commissioner as to the purposes of journalism or artistic or literary purposes.
- 80. Restriction on enforcement in case of processing for the purposes of journalism or for artistic or literary purposes.
- 81. Failure to comply with notice.
- 82. Service of notice by Commissioner.
- 83. Warrants.
- 84. Execution of warrants.
- 85. Matters exempt from inspection and seizure.
- 86. Return of warrants.

## *Data Protection*

---

87. Obstruction of execution of a warrant.

### PART X

#### *Data Protection Tribunal*

88. Establishment of the Data Protection Tribunal.  
89. Right of appeal.  
90. Determination of appeals.

### PART XI

#### *Miscellaneous*

91. Right to compensation and liability.  
92. Unlawful obtaining of personal data.  
93. Disclosure of information.  
94. Act binds Crown.  
95. Amendment of Schedule.  
96. Regulations.  
97. Commencement.

### SCHEDULE

**BELIZE:**

**BILL**

**For**

**AN ACT** to regulate the collection, keeping, use and dissemination of personal data; to protect the privacy of individuals in relation to their personal data; and to provide for matters connected therewith or incidental thereto.

*(Gazetted ....., 2021)*

**BE IT ENACTED**, by and with the advice and consent of the House of Representatives and Senate of Belize and by the authority of the same, as follows:

**PART I**

*Preliminary*

**1.** This Act may be cited as the

Short title.

**DATA PROTECTION ACT, 2021.**

**2.** In this Act—

Interpretation.

“accessible public record” means any record that is kept by a public authority and to which members of the public are given access;

“accessible record” means—

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

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

“child” means a person who is under the age of 16 years;

“Commissioner” means the Data Protection Commissioner referred to in section 68;

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

“data” means information that–

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;
- (b) is recorded with the intention that it should be processed by means of such equipment;
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system;
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record; or
- (e) does not fall within paragraph (a), (b), (c) or (d) but is recorded information held by a public authority;

“data controller” means–

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

“data privacy officer” means a person designated as such pursuant to section 65;

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

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

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



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

“health care professional” includes a person who is registered under any health care provider legislation;

“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;

“Minister” means the Minister responsible for digital transformation, e-governance or information technology;

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

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

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

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

- (a) organization, adaptation or alteration of the information or data;
- (b) retrieval, consultation or use of the information or data;

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

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

- (a) racial or ethnic origin;
- (b) political opinions;

## *Data Protection*

---

- (c) religious beliefs or other beliefs of a similar nature;
- (d) membership of a political body;
- (e) membership of a trade union;
- (f) genetic data;
- (g) biometric data;
- (h) sexual orientation or sexual life;
- (i) financial record or position;
- (j) criminal record; or
- (k) proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court of competent jurisdiction in such proceedings;

“small business” means a business at a time (the test time) in a financial year (the current year) if its annual turnover for the previous financial year is \$3,000,000 or less;

CAP. 300.

“trade union” has the meaning assigned to it under section 2 of the Trade Unions Act;

“Tribunal” means the Data Protection Tribunal established under section 88.

Application of  
Act.

**3.—(1)** This Act applies to—

- (a) the processing of personal data in the context of the activities of a data controller or a data processor established in Belize; and
- (b) the processing of personal data of data subjects in Belize by a data controller or a data processor not established in Belize, where the processing activities are related to the offering of goods or services to data subjects in Belize.

(2) For the purposes of sub-section (1) a data controller or data processor is established in Belize if that data controller or data processor is—

- (a) an individual who is ordinarily resident in Belize;

- (b) a body, association or other entity incorporated, organised, registered or otherwise formed under the laws of Belize; or
  - (c) a person who does not fall within paragraph (a) or (b) but maintains in Belize an office, branch or agency through which he carries on any activity related to the processing of personal data.
- (3) Notwithstanding sub-sections (1) and (2), small businesses are exempted from the application of this Act except for a small business—
- (a) providing health service;
  - (b) trading in personal information;
  - (c) an operator of a residential tenancy database;
  - (d) a credit reporting body;
  - (e) a reporting entity for the purposes of the Money Laundering and Terrorism (Prevention) Act Cap. 104
  - (f) employee associations registered or recognised under any enactment in Belize;
  - (g) a business prescribed by under regulations made under this Act;
  - (h) a business that has opted in to be covered by this Act.

## PART II

### *Data Protection Principles*

#### 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 shall not be further processed in a manner that is incompatible with those purposes;
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- (d) accurate and, where necessary, kept up to date and reasonable steps shall be taken to ensure that personal data

Principles  
relating to  
processing of  
personal data.

that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; and
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(2) In determining whether any disclosure of personal data is compatible with the purpose for which the data is obtained in accordance with sub-section (1)(b), regard shall be had to the purpose for which the personal data is intended to be processed by any person to whom the data is disclosed.

(3) Pursuant to sub-section (1)(f), having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to—

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

Duty of data controller to comply with principles.

**5.—**(1) A data controller shall, in relation to all of the personal data he processes, comply with the principles under section 4 and where requested by the Commissioner, demonstrate compliance with those principles.

(2) A data controller may specify the purpose for which personal data is obtained pursuant to section 4(1)(b)—

- (a) in any information given for the purposes of section 6(3)(a) by the data controller to the data subject; or
- (b) in a notification given to the Commissioner under Part III.

(3) Section 4 (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.

(4) A data controller shall take reasonable steps to ensure that his employees who have access to the personal data comply with the principles set out in section 4(1).

(5) Pursuant to section 4 (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).

(6) 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 section 4 (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 section 4 (1)(f).

(7) A person who fails to comply with the requirements set out under this section (1) commits an offence and is liable on summary conviction to a fine of five hundred thousand dollars or to imprisonment for three years or to both such fine and term of imprisonment.

Fairness of  
processing.

**6.—(1)** In determining whether personal data is processed fairly in accordance with section 4 (1)(a), regard shall 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 sub-section (3), personal data shall be treated as having been obtained fairly if the personal data consists of information obtained from a person who is—

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

(3) Personal data shall not to be treated as processed fairly unless—

- (a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has readily available to him, the following information—
  - (i) the identity of the data controller;
  - (ii) where a data controller has nominated a representative for the purposes of this Act, the identity of that representative;
  - (iii) the purpose for which the data is intended to be processed; and
  - (iv) any further information which is necessary, having regard to the specific circumstances in which the data is or is to be processed, to enable processing in respect of the data subject to be fair; and
- (b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject is provided with, or has readily available to him, the information specified in paragraph (a).

(4) For the purposes of sub-section (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.

**7.—(1)** For the purposes of section 4(1)(a), processing shall be lawful where—

Lawfulness of  
processing

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

## *Data Protection*

---

- (x) for the purposes of the legitimate interests pursued by the data controller or by any 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) Sub-section (1)(b)(x) shall not apply to processing carried out by public authorities in the performance of their tasks.

Conditions for consent.

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

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

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

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

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

Conditions applicable to child's consent.

**9.**—(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—

- (a) the parent or guardian of the child; or
- (b) the child where the child is over the age of thirteen.

(2) A child shall receive the same privacy protections and rights as an adult.

**10.**—(1) Processing of sensitive personal data shall be prohibited unless—

- (a) the data subject gives consent to the processing;

Processing of sensitive personal data.



- (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 a body or association which—
    - (A) is not established or conducted for profit; and
    - (B) exists for political, philosophical, religious or trade union purposes;
  - (ii) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
  - (iii) relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and
  - (iv) does not involve disclosure of the personal data to a third party without the consent of the data subject;
- (f) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject;
- (g) the processing is necessary—
  - (i) for the purpose of, or in connection with, any legal proceedings, including prospective legal proceedings;

- (ii) for the purpose of obtaining legal advice; or
  - (iii) for the purpose of establishing, exercising or defending legal rights;
- (h) the processing is necessary for the administration of justice;
- (i) the processing is necessary for the exercise of any functions of either House of the National Assembly;
- (j) the processing is necessary for the exercise of any functions conferred on any person by or under an enactment;
- (k) the processing is necessary for the exercise of any functions of a public authority;
- (l) the processing is necessary for medical purposes and is undertaken by—
  - (i) a health care professional; or
  - (ii) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health care professional;
- (m) the processing—
  - (i) is of sensitive personal data consisting of information as to racial or ethnic origin; and
  - (ii) is necessary for the purpose of identifying or keeping under review, the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
  - (iii) is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2) The processing of personal data relating to criminal convictions and offences or related security measures shall be carried out only under the control of an official authority responsible for processing such personal data or when the processing is authorised by any enactment providing for appropriate safeguards for the rights and freedoms of data subjects.

(3) Any comprehensive register of criminal convictions shall be kept only under the control of an official authority.

(4) For the purposes of sub-section (1)(l) “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health care services.

### PART III

#### *Rights of a Data Subject*

Right of access.

**11.—(1)** A data subject has the right—

- (a) to be informed by a data controller whether personal data of that data subject is being processed by or on behalf of the data controller;
- (b) where personal data of the data subject is being processed by or on behalf of the data controller, to request from, and to be given by, the data controller, a description of—
  - (i) the purposes of the processing;
  - (ii) the categories of personal data concerned;
  - (iii) the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular recipients in other countries or international organisations;
  - (iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
  - (v) the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
  - (vi) the right to lodge a complaint with the Commissioner;
  - (vii) any available information as to their source, where the personal data is not collected from the data subject;
  - (viii) the existence of automated decision-making, including profiling, referred to in section 19 and, at least in those cases, meaningful information about the logic

## *Data Protection*

---

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) A 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 a 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 sub-section (3) shall not adversely affect the rights and freedoms of other data subjects.

Right to  
rectification.

**12.**—(1) A data subject shall have the right to obtain from a data controller, without undue delay, the rectification of inaccurate personal data concerning the data subject.

(2) Taking into account the purposes of the processing, a data subject shall have the right to have incomplete personal data completed by a data controller and to be provided with a copy of the updated personal data.

Right to erasure.

**13.**—(1) A data subject shall have the right to obtain from a data controller the erasure of personal data concerning him without undue delay.

(2) A 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 7(1)(a) or section 10(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;
- (e) the personal data has to be erased in compliance with a legal obligation in Belize to which the data controller is subject.

(3) Where a data controller has made personal data public and is obliged pursuant to sub-section (1) or (2) to erase the personal data, the data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data controllers who are processing the personal data that the data subject has requested the erasure by such data controllers of any links to, or copy or replication of, the personal data.

(4) Sub-sections (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 enactment to which the data controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- (c) 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.

**14.—(1)** A data subject shall have the right to obtain from a data controller, restriction of processing of personal data where one of the following applies—

Right to  
restriction of  
processing.

- (a) the accuracy of the personal data is contested by the data subject;
- (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- (c) the data controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- (d) the data subject has objected to processing pursuant to section 17 pending the verification whether the legitimate

## *Data Protection*

---

grounds of the data controller override those of the data subject.

(2) A restriction of processing under sub-section (1)(a) may be for a period enabling the data controller to verify the accuracy of the personal data;

(3) Where processing has been restricted under sub-section (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 in Belize.

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

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

**15.—(1)** A data controller shall communicate to every recipient to whom the personal data of a data subject 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) A data controller shall inform the data subject about the recipients to whom personal data has been disclosed if the data subject requests such information.

Right to data  
portability.

**16.—(1)** A data subject has the right to receive his personal data he provided to a data controller, in a structured, commonly used and machine-readable format.

(2) A data subject has the right to transmit his personal he provided to a data controller to another data controller without hindrance where—

- (a) the processing is based on consent pursuant to section 7(1)(a) or section 10(1)(a) or on a contract pursuant to section 7(1)(b)(i); and

(b) the processing is carried out by automated means.

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

(4) The exercise of the right referred to in sub-section (1) shall be exercised without prejudice to section 13.

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

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

**17.—(1)** Subject to sub-section (2), a data subject may, by a written notice to a data controller, require that data controller, at the end of a twenty one day period to, cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, any personal data of the data subject, on the ground that—

Right to prevent processing likely to cause damage or distress.

(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) Sub-section (1) shall not apply—

(a) in a case where any of the conditions in section 7(1) (a) or (b)(i), (ii), (iii) or (iv) is satisfied; or

(b) in such other cases as the Minister may prescribe by Order published in the *Gazette*.

(3) A data controller shall, within twenty one days of receiving a notice under sub-section (1), give the data subject written notice stating—

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

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

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

(4) Where the Supreme Court is satisfied, on the application of a data subject who has given notice under sub-section (1), that a data controller has failed to comply with the notice, the Court may order the data controller to take such steps for complying with the notice as the Court sees fit.

Right to prevent processing for purposes of direct marketing.

**18.—(1)** A data subject may, by written notice to a data controller, require the data controller at the end of a twenty one day period to cease processing for the purposes of direct marketing, personal data of the data subject.

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

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

Automated individual decision-making, including profiling.

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

(2) Sub-section (1) shall not apply where the automated processing or profiling of personal data is—

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

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

(4) Sub-section (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.



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

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

- (a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- (b) the contact details of the data privacy officer, where applicable;
- (c) the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- (d) where the processing is done pursuant to section 7(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;

(2) In addition to the information referred to in sub-section (1), a data controller shall at the time when personal data is obtained, provide the data subject with the following 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 7(1)(a) or section 10(1)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- (d) the right to lodge a complaint with the Commissioner;
- (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

- (f) the existence of automated decision-making, including profiling, referred to in section 19 and 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 the further processing of the personal data, with information on that other purpose and with any relevant further information as referred to in sub-section (2).

(4) Sub-sections (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, a data controller shall provide the data subject with the following—

- (a) the identity and the contact details of the data controller and, where applicable, of the data controller's representative;
- (b) the contact details of the data privacy officer, where applicable;
- (c) the purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
- (d) the categories of personal data concerned;
- (e) the recipients or categories of recipients of the personal data, if any;

(1) A data controller shall provide a 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 7(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 7(1)(a) or section 10(1)(a), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
  - (e) the right to lodge a complaint with the Commissioner;
  - (f) from the source from which originated the personal data, and if applicable, whether it came from publicly accessible sources;
  - (g) the existence of automated decision-making, including profiling, referred to in section 19 and 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 sub-sections (1) and (2)–
  - (a) within a reasonable period after obtaining the personal data, but not later than one month after obtaining the personal data, 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, not later than the time of the first communication to the data subject; or
  - (c) if a disclosure to another recipient is envisaged, not later than when the personal data is first disclosed to another recipient.
- (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 further processing the personal data, with information on that other purpose and with any relevant further information as referred to in sub-section (2).
- (5) Sub-sections (1), (2), (3) and (4) shall not apply where–
  - (a) the data subject already has the information;
  - (b) the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes pursuant to section 36;
  - (c) obtaining of disclosure is expressly laid down by any enactment to which the data controller is subject and which

provides appropriate measures to protect the data subject's legitimate interests; or

- (d) where the personal data must remain confidential subject to an obligation of professional secrecy regulated by any enactment.

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

**22.—(1)** A 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 59 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

(2) The information pursuant to sub-section (1) shall be provided in writing, or by other means, including, where appropriate, by electronic means.

(3) When requested by a data subject, a data controller may provide the information, pursuant to the rights of the data subject under sections 11 to 16 and section 19, orally.

(4) Prior to providing information orally, a data controller shall verify the identity of the data subject.

(5) A data controller shall facilitate the exercise of data subject rights under sections 11 to 16 and 19.

(6) A data controller shall provide information on action taken on a request under sections 11 to 16 and 18 to the data subject without undue delay and in any event within one month of receipt of the request.

(7) The period of time referred to in sub-section (6) may be extended by two months where necessary, taking into account the complexity and number of the requests under sections 11 to 16 and 18.

(8) A data controller shall inform a data subject of any extension granted pursuant to sub-section (7) within one month of receipt of the request, together with the reasons for the delay.

(9) Where a data subject makes a request pursuant to his rights under sections 11 to 16 and 18 by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

(10) Where a data controller does not take action on the request of a data subject under this section, the data controller shall inform the data

subject, without delay and not later than one month of receipt of the request, of—

- (a) the reasons for not taking action; and
- (b) on the possibility of lodging a complaint with the Commissioner or appealing to the Supreme Court.

(11) Information provided under sections 19 and 20 and any communication and any action taken under sections 11 to 16, 19 and 59, shall be provided free of charge.

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

- (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.

(13) A data subject may object to the decision of a data controller made pursuant to sub-section (12) by lodging a complaint with the Commissioner or appealing to the Tribunal.

(14) A data subject may be represented by a not-for-profit organisation when making complaints and pursuing appeals under this Act.

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

(16) Where a data controller has reasonable doubts concerning the identity of an 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.

(17) 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 they shall be machine-readable.

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

PART IV

*Transfers of Personal Data out of Belize*

General principle  
for transfers.

**23.**—(1) Where personal data is transferred to a country or territory outside Belize, the transferor shall ensure there is—

- (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 that there are effective legal remedies available for data subjects.

(2) Notwithstanding sub-section (1) nothing in this Act prevents the transfer of data from Belize to a country or territory outside Belize for the purposes of cloud storage and consent of any data subject is not required for transfer of data from Belize to a country or territory outside Belize for the purposes of cloud storage.

Adequate level  
of protection.

**24.** For the purposes of section 23(a), an adequate level of protection is one which is adequate in all the circumstances of the case, having regard 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 the data is intended to be processed;
- (e) the period during which the data is intended to be processed;
- (f) the law in force in the country or territory in question;
- (g) the international obligations of that country or territory;
- (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.

**25.** For the purposes of section 23(b), appropriate safeguards may be provided for by—

Appropriate  
safeguards.

- (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 a data controller or data processor and a data controller, data processor or the recipient of 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.

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

Binding  
corporate rules.

- (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 Belize;
- (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 Supreme 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 a data controller or data processor of liability for any breaches of the binding corporate rules;
- (g) that the data controller or the data processor shall be exempt from the liability referred to in paragraph (f), in whole or in part, only where it is proven that the data controller or data processor is not responsible for the event giving rise to the damage;
- (h) how the information on the binding corporate rules is provided to the data subjects;
- (i) the complaint procedures;
- (j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules;
- (k) the mechanisms for reporting and recording changes to the binding corporate rules and reporting those changes to the supervisory authority;
- (l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority or Commissioner the results of verifications of the measures specified in paragraph (j);
- (m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject, which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and
- (n) the appropriate data protection training to personnel having permanent or regular access to personal data.

(2) Binding corporate rules referred to in sub-section (1) shall be submitted to the Commissioner for authorisation.



(3) A code of conduct or certification mechanism shall be put in place by which a data controller can demonstrate appropriate technical and organisational measures.

(4) 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.

(5) For the purposes of this section—

- (a) “binding corporate rules” means personal data protection policies which are adhered to by a data controller or data processor for transfers or a set of transfers of personal data to a data controller or a data processor in one or more countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;
- (b) “enterprise” means a person engaged in an economic activity;
- (c) “supervisory authority” means an independent public authority which is established in a country or territory outside of Belize.

**27.** The principles for transfers under section 23 shall not apply where—

*Derogations.*

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

## *Data Protection*

---

- (v) reasons of substantial public interest;
  - (vi) the purpose of, or in connection with, any legal proceedings including prospective legal proceedings;
  - (vii) the purpose of obtaining legal advice;
  - (viii) the purposes of establishing, exercising or defending legal rights; or
  - (ix) the protection of the vital interests of the data subject;
- (c) the transfer of personal data is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data is or may be disclosed after the transfer;
- (d) the transfer of personal data is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects; or
- (e) the transfer of personal data has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

Non-compliance. **28.** A person who contravenes sections 23 commits an offence and is liable on summary conviction to a fine of twenty thousand dollars.

Substantial public interest. **29.—(1)** The Minister may by Order published in the *Gazette*, specify the—

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

(2) An Order made pursuant to sub-section (1) shall be subject to negative resolution.

PART V

*Exemptions*

**30.—(1)** In this Part—

References to subject information provisions and non-disclosure provisions.

(a) “subject information provisions” refers to—

(i) section 4(1)(a) to the extent to which it requires compliance with section 6(2); and

(ii) section 11;

(b) “non-disclosure provisions” refers to the following provisions to the extent to which they are inconsistent with the disclosure in question—

(i) section 4(1)(a), except to the extent to which it requires compliance with the conditions in sections 7 and 10;

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

(iii) sections 12 to 19.

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

**31.** Parts II, III, IV, VII and section 77 shall not apply where the processing of personal data is required for the purpose of safeguarding national security.

National Security.

**32.—(1)** Personal data processed for—

Crime and taxation

(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 7 and 10, 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 possession for any of the purposes mentioned in sub-section (1) (a) to (c),

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

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

- (a) the disclosure is for any of the purposes mentioned in sub-section (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 sub-section (1)(a) to (c).

(4) Personal data in respect of which a data controller is a public authority and which—

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

is exempt from section 11 to the extent to which the exemption is required in the interests of the operation of the system.

Health,  
education and  
social work.

**33.—(1)** The Minister may, by Order published in the *Gazette*, exempt from subject information provisions, or modify subject information provisions in relation to, personal data—

- (a) consisting of information as to the physical or mental health or condition of a data subject;

- (b) in respect of which the data controller is an educational institution and which consists of information relating to persons who are or have been pupils at the educational institution;
- (c) in respect of which the data controller is a tertiary institution and which consists of information relating to persons who are or have been students at the tertiary institution;
- (d) of such other description 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 sub-section (1)(d), the Minister shall not confer any exemption or make any modification under sub-section (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.

**34.**—(1) Personal data processed for the purposes of discharging functions to which this section applies is exempt from subject information provisions to the extent to which the application of those provisions to the data would be likely to prejudice the proper discharge of those functions.

Regulatory activity.

(2) Sub-section (1) applies to any relevant function which is designed for the purpose of—

- (a) protecting members of the public against—
  - (i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate;
  - (ii) financial loss due to the conduct of discharged or undischarged bankrupts; or
  - (iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons authorised to carry on any profession or other activity;

- (b) protecting charities against misconduct or mismanagement, whether by trustees or other persons in their administration;
- (c) protecting the property of charities from loss or misapplication;
- (d) the recovery of the property of charities;
- (e) securing the health, safety and welfare of persons at work; or
- (f) protecting persons other than persons at work against risk to health or safety arising out of, or in connection with, the actions of persons at work.

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

- (a) maladministration by public authorities;
- (b) failures in services provided by public authorities; or
- (c) a failure of a public authority to provide a service which it is a function of the authority to provide,

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

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

- (a) protecting members of the public against conduct which may adversely affect their interests by persons carrying on a business;
- (b) regulating agreements or conduct which have as their object or effect the prevention, restriction or distortion of competition in connection with any commercial activity; or
- (c) regulating conduct on the part of one or more undertakings which amounts to the abuse of a dominant position in a market,

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

(5) For the purposes of sub-section (2) “relevant function” means—

- (a) any function conferred on any person by or under any enactment;
- (b) any function of a public authority; or
- (c) any other function which is of a public nature and is exercised in the public interest.

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

Journalism,  
literature and art.

- (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 to the special importance of the public interest in freedom of expression, publication would be in the public interest; and
- (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the purpose of journalism or artistic or literary purposes.

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

(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 for artistic or literary purposes; and
- (b) with a view to the publication by any person of any journalistic, literary or artistic material which, at the time 24 hours immediately before the relevant time, had not previously been published by the data controller,

the proceedings shall be stayed until either of the conditions in sub-section (4) are met.

(4) The conditions referred to in sub-section (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 sub-sections (1) to (3), personal data is not to be treated as processed otherwise than for research purposes merely because the data is disclosed—

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

(5) In this section—

- (a) “research purposes” includes statistical or historical purposes;
- (b) “the relevant conditions” means the conditions that the data—



## *Data Protection*

---

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

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

Manual data held by public authorities.

**38.** Personal data is exempt from Parts II, III, IV and VI where the data consists of information which the data controller is obliged by or under any enactment to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

Information available to the public by or under enactment.

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

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

(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.

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

Parliamentary privilege.

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

Legal professional privilege.

**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.

Domestic purposes.

**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—

Confidential references given by the data controller.

- (a) the education, training or employment, or prospective education, training or employment, of the data subject;

## *Data Protection*

---

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

Armed forces

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

Judicial appointments and honours

**45.** Personal data processed for the purposes of—

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

is exempt from the subject information provisions.

Appointments to public service.

**46.** The Minister may by Order published in the *Gazette*, exempt from the subject information provisions personal data processed for the purposes of assessing any person's suitability for—

- (a) employment in the public service; or
- (b) any office to which appointments are made by the Governor-General or by a Minister.

Corporate finance.

**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 subject information provisions to the extent to which either—
  - (i) the application of those provisions to the data could affect the price of any instrument which is already in existence or is to be or may be created; or
  - (ii) the data controller reasonably believes that the application of those provisions to the data could affect the price of any such instrument; and
- (b) to the extent that the data is not exempt from the subject information provisions by virtue of paragraph (a), the data is exempt from those provisions where the exemption is required for the purpose of safeguarding an important economic or financial interest of Belize.

(2) For the purposes of sub-section (1)(b) the Minister may by Order published in the *Gazette* specify—

- (a) matters to be taken into account in determining whether exemption from the subject information provisions is required for the purpose of safeguarding an important economic or financial interest of Belize; 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—

- (a) “corporate finance service” means a service consisting of—
  - (i) underwriting in respect of issues of, or the placing of issues of, any instrument;
  - (ii) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings; or
  - (iii) services relating to such underwriting as is mentioned in paragraph (a); and
- (b) “price” includes value.

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

Negotiations  
with data  
subject.

**49.—(1)** The results of an examination are exempt from section 11.

Examinations.

(2) Personal data consisting of information recorded by candidates during an academic, professional or other examination is exempt from section 11.

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

**50.—(1)** The Minister may, by Order published in the *Gazette*, exempt from the subject information provisions personal data consisting of information, the disclosure of which is prohibited or restricted by or under

Powers to make  
further  
exemptions by  
order.

## *Data Protection*

---

any enactment, where and to the extent that he considers it necessary for the prohibition or restriction to prevail for the purpose of safeguarding—

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

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

(3) Any Order made under this section shall be subject to negative resolution.

## PART VI

### *Data Sharing*

**51.**—(1) In accordance with the provisions of this Part, agencies are authorised to share personal information in accordance with an approved information sharing agreement to facilitate the provision of public services.

Agencies to  
share  
information.

- (2) An information sharing agreement may—
- (a) duplicate an information sharing provision by providing for an agency to share the same personal information specified in the information sharing provision—
    - (i) with the same agencies specified in the information sharing provision; and
    - (ii) for the same purposes specified in the information sharing provision; or
  - (b) extend an information sharing provision that is not a restricted information sharing provision by providing for an agency to share the same personal information specified in the information sharing provision—
    - (i) with the same agencies specified in the information sharing provision for a purpose not specified in the information sharing provision;

- (ii) with an agency not specified in the information sharing provision for a purpose specified in the information sharing provision; or
    - (iii) with an agency not specified in the information sharing provision and for a purpose not specified in the information sharing provision; or
  - (c) duplicate a restricted information sharing provision by providing for an agency to share the same personal information as specified in the restricted information sharing provision—
    - (i) with the same agencies specified in the restricted information sharing provision; and
    - (ii) for the same purposes specified in the restricted information sharing provision; or
  - (d) extend in any manner specified in paragraph (b) a restricted information sharing provision, but only if—
    - (i) the restricted information sharing provision is an information matching provision; or
    - (ii) there is express statutory authorisation to do so.
- (3) In this section—
  - (a) “information sharing provision” means a provision in any enactment other than this Act that authorises or requires the sharing of personal information by an agency with one or more other agencies for one or more specified purposes;
  - (b) “restricted information sharing provision” means an information sharing provision that expressly restricts the purposes for which the personal information may be shared to those purposes specified.

**52.** For the avoidance of doubt, nothing in this Part—

- (a) limits the collection, use, or disclosure of personal information that is authorised or required by or under any enactment; or
- (b) compels agencies to enter into an information sharing agreement if those agencies are already allowed to share personal information—

Relationship between this Part and other law relating to data disclosure.

- (i) by or under any other enactment; or
- (ii) because an exemption from or a modification to one or more of the Data Privacy Principles or any code of practice is not required to make the sharing of the information lawful.

## PART VII

### *Data Controller and Data Processor*

Compliance. **53.**—(1) A data controller shall demonstrate compliance with the mechanisms in this Part which the data controllers use to identify, assess and mitigate risks to personal data.

(2) A data controller or data processor shall abide with any code of conduct made under section 72 or any certification mechanism put in place by which a data controller can demonstrate appropriate technical and organisational measures.

Responsibility of the data controller. **54.**—(1) A 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 sub-section (1) shall include the implementation of appropriate data protection policies by the data controller.

Data protection by design and by default. **55.**—(1) A data controller shall, at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures designed to implement the principles set out in section 4 in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Act and protect the rights of data subjects, taking into consideration the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing.

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

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

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

**56.**—(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 shall—

Data Processor.

- (a) be in accordance with the requirements of this Act; and
- (b) ensure the protection of the rights of the data subject.

(2) A 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 sub-section (2), a data processor shall inform the data controller of any intended changes concerning the addition or replacement of other data processors and the data controller shall be given the opportunity to object to such changes.

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

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

(5) A contract prepared pursuant to sub-section (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 Belize or an international organisation, unless required to do so by any enactment and in such a case, the data processor shall inform the data controller of that legal requirement before processing, unless the enactment prohibits such information to be shared on 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 58.
- (d) respects the conditions referred to in sub-sections (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 58 to 62, taking into account the nature of processing and the information available to the data processor;
- (g) on the determination of the data controller, deletes or returns all the personal data to the data controller after the end of the provision of services relating to processing, and deletes existing copies unless the enactment requires storage of the personal data;
- (h) makes available to the data controller all information necessary to demonstrate compliance with the obligations set out in this section and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

(6) Where in relation to sub-section (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 sub-section (2), the same obligations as set out in the contract between the data controller and the data processor as referred to sub-sections (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 sub-section (7) fails to fulfil its data protection obligations, the initial data processor referred to in sub-section (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 sub-sections (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.

**57.**—(1) A 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 that data except on instructions from the data controller, unless required to do so by any enactment.

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

(2) A person who contravenes sub-section (1) commits an offence and is liable on summary conviction to a fine of twenty thousand dollars .

**58.**—(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 the following—

Records of processing activities.

- (a) the name and contact details of the data controller and, where applicable, any joint data controller, the data controller's representative and the data privacy officer;
- (b) the purposes of the processing;
- (c) a description of the categories of data subjects and of the categories of personal data;
- (d) the categories of recipients to whom the personal data has been or will be disclosed including recipients in other countries or international organisations;
- (e) where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in section 27, the documentation of suitable safeguards;
- (f) where possible, the envisaged time limits for erasure of the different categories of data;

## *Data Protection*

---

- (g) where possible, a general description of the technical and organisational security measures referred to in section 58(1).

(2) A data processor and, where applicable, the data processor's representative, shall maintain a record of all categories of processing activities carried out on behalf of a data controller, which contains—

- (a) the name and contact details of the data processor or data processors and of each data controller on behalf of whom the data processor is acting, and, where applicable, of the data controller's or the data processor's representative, and the data privacy officer;
- (b) the categories of processing carried out on behalf of each data controller;
- (c) where applicable, transfers of personal data to another country or an international organisation, including the identification of that country or international organisation and, in the case of transfers referred to in section 27, the documentation of suitable safeguards;
- (d) where possible, a general description of the technical and organisational security measures referred to in section 58(1).

Cooperation with  
the  
Commissioner.

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

Security of  
processing.

**60.—(1)** Taking into account 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, a data controller and a 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) A data controller and data processor shall take steps to ensure that any individual acting under the authority of that data controller or data processor who has access to personal data does not process the personal data except on instructions from the data controller, unless he is required to do so by any enactment.

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

Notification of a personal data breach to the Commissioner.

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

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

(4) A notification of a personal data breach to the Commissioner referred to in sub-section (1) shall—

- (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- (b) communicate the name and contact details of the data privacy officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach; 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 all the information required under sub-section (4) at the same time, the information may be provided in phases.

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

Communication  
of a personal  
data breach to  
the data subject.

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

(2) A notification under sub-section (1) shall describe in clear and plain language the nature of the personal data breach and contain the information referred to in section 61(4)(b), (c) and (d).

(3) A notification under sub-section (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 sub-section (1) is no longer likely to materialise;
- (c) it would involve disproportionate effort and in such a case, there shall be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Data protection  
impact  
assessment.

**63.**—(1) Where a type of processing, in particular processing using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of

an individual, a data controller shall, prior to the processing, carry out a data protection impact assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) A data protection impact assessment pursuant to sub-section (1) may address a set of similar processing operations that present similar high risks.

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

(4) A data protection impact assessment referred to in sub-section (1) shall in particular be required in the case of—

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

(5) The Commissioner shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to sub-section (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 sub-section (1) shall contain—

- (a) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
- (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- (c) an assessment of the risks to the rights and freedoms of data subjects referred to in sub-section (1); and

- (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.

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

(9) Where necessary, a 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.

**64.—(1)** A data controller shall consult the Commissioner prior to processing, where a data protection impact assessment under section 63 indicates that the processing would result in a high risk to the rights and freedoms of an individual in the absence of measures taken by the data controller to mitigate the risk.

(2) Where the Commissioner is of the opinion that the intended processing referred to in sub-section (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 under sub-section (2) may be extended up to 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 extension within one month of receipt of the request for consultation together with the reasons for the delay.

(5) The period mentioned under sub-section (2) may be suspended until the Commissioner has obtained information he has requested for the purposes of the consultation.

(6) When consulting the Commissioner pursuant to sub-section (1), the data controller shall provide the Commissioner with—

- (a) where applicable, the respective responsibilities of the data controller and data processors involved in the processing, in particular for processing within a group of undertakings;

- (b) the purposes and means of the intended processing;
- (c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Act;
- (d) where applicable, the contact details of the data privacy officer;
- (e) the data protection impact assessment provided for in section 63;
- (f) any other information requested by the Commissioner.

**65.**—(1) A data controller and data processor shall designate a data privacy officer in any case where—

Designation of the data privacy officer.

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

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

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

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

(5) A data privacy officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the duties and functions referred to in section 67.

## *Data Protection*

---

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

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

Position of the  
data privacy  
officer.

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

(2) A data controller and data processor shall support the data privacy officer in performing the duties and functions referred to in section 67, by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his expert knowledge.

(3) A data privacy officer shall not be dismissed or penalised by the data controller or the data processor for performing duties and functions referred to in section 67.

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

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

(6) A data privacy officer is required to keep confidential all matters concerning the performance of his duties and functions referred to in section 67.

Duties and  
functions of a  
data privacy  
officer.

**67.—(1)** A data privacy officer shall—

- (a) inform and advise the data controller or the data processor and the employees who carry out processing of their obligations pursuant to this Act;
- (b) monitor compliance with this Act and with the policies of the data controller or data processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- (c) provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to section 63;



- (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 64, and to consult, where appropriate, with regard to any other matter.

(2) A data privacy officer shall in the performance of his duties and functions under this section have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

## PART VIII

### *Data Protection Commissioner*

**68.**—(1) There shall be a public officer in the Ministry responsible for digital transformation, e-governance or information technology, to be called the Data Protection Commissioner, who shall be responsible for the general administration of this Act.

Data Protection  
Commissioner.

(2) A person is qualified to hold or to act in the post of Data Protection Commissioner, where that person has specializations or experience in the fields of law, cyberlaw, telecommunications law, economics, finance, information security or technology for periods amounting in the aggregate to not less than seven years.

(3) The Data Protection Commissioner shall at all times act independently and remain free from external influence.

**69.** Without prejudice to the generality of the functions set out in this Act, the Commissioner shall perform the following functions—

Functions of  
Commissioner.

- (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 the obligations of data controllers and data processors under this Act;
- (d) organise activities addressed specifically to children to educate them about the risks, rules, safeguards and rights in relation to processing;
- (e) conduct, at his own discretion or where requested to do so by any person, an audit of the personal data processed by the

## *Data Protection*

---

person, for the purpose of ascertaining whether or not the data is processed in accordance with this Act;

- (f) upon request, provide information to any data subject concerning the exercise of their rights under this Act;
- (g) monitor the processing of personal data and, in particular, sensitive personal data, and any other matter affecting the privacy of persons in respect of their personal data, and—
  - (i) report to the Minister on the results of that monitoring; and
  - (ii) where appropriate, make recommendations on the need for, or desirability of, taking legislative, administrative or other action to give protection or better protection, to the privacy of persons in respect of their personal data;
- (h) examine any proposed legislation or proposed policy of the Government that—
  - (i) the Commissioner considers may affect the privacy of persons in respect of their personal data; or
  - (ii) provides for the collection of personal data by any public authority or the disclosure of personal data by one public authority to another public authority,and report to the Minister the results of that examination;
- (i) conduct investigations on the application of this Act, including on the basis of information received from a public authority;
- (j) receive and invite representations from members of the public on any matter affecting the privacy of persons in respect of their personal data;
- (k) consult and cooperate with other persons concerned with the privacy of persons in respect of their personal data;
- (l) make suggestions to any person in relation to any matter that concerns the need for, or the desirability of, action by that person in the interest of the privacy of persons in respect of their personal data;

- (m) provide, at his own discretion or where requested to do so, advice to any Minister, public authority or person on any matter relevant to the operation of this Act;
- (n) inquire generally into any matter, including any law, practice or procedure, whether governmental or non-governmental, or any technical development, where it appears to the Commissioner that the privacy of persons in respect of their personal data is being or may be infringed thereby;
- (o) undertake research into, and monitor developments in, data processing and computer technology to ensure that any adverse effects of such developments on the privacy of persons in respect of their personal data is minimised, and report to the Minister the results of such research and monitoring;
- (p) report to the Minister on the desirability of the acceptance, by Belize, of any international instrument relating to the privacy of persons in respect of their personal data;
- (q) monitor relevant developments, insofar as they have an impact on the protection of personal data, in particular the development of information and communication technologies and commercial practices;
- (r) prepare appropriate codes of practice for the guidance of persons processing personal data;
- (s) recommend the adoption and development of standard contractual clauses and standard data protection clauses pursuant to this Act;
- (t) establish and maintain a list in relation to the requirement for data protection impact assessment pursuant to section 63(5) and (6);
- (u) investigate complaints from persons concerning abuses in the processing of personal data;
- (v) approve binding corporate rules pursuant to section 26;
- (w) keep internal records of contraventions of this Act and of measures taken to address those contraventions;
- (x) do anything incidental or conducive to the performance of any of the preceding functions; and

## *Data Protection*

---

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

Staff.

**70.**—(1) There shall be appointed by the Public Services Commission to assist the Commissioner in the discharge of his functions such number of public officers as may be required.

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

Confidential  
information.

**71.**—(1) The Commissioner and a public officer appointed pursuant to section 70(1) shall keep secret all confidential information coming to his knowledge during the course of the administration of this Act or any other Act that the Commissioner has jurisdiction to administer or enforce, except insofar as disclosure is necessary for the administration of this Act or insofar as the Commissioner authorises that person to release the information.

(2) Sub-section (1) shall not apply where disclosure is required pursuant to—

- (a) an order made by a court of competent jurisdiction;
- (b) a duty or obligation imposed by any enactment; or
- (c) an international agreement to which Belize is a party.

(3) A person who contravenes sub-section (1) commits an offence and is liable on summary conviction to a fine of twenty thousand dollars .

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

Indemnity.

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

**73.**—(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 Commissioner throughout the preceding financial year in such detail as the Minister may direct. Report.

(2) A copy of the report of the Commissioner referred to in sub-section (1) shall be printed and laid before both Houses of the National Assembly and published in the *Gazette* not later than three months from the date of receipt by the Minister.

## PART IX

### *Enforcement*

**74.**—(1) Where the Commissioner is satisfied that a data controller or a data processor has contravened this Act, the Commissioner may serve him with an Enforcement Notice, requiring the data controller or data processor, as the case may be, to— Enforcement notice.

- (a) take, within such time as may be specified in the notice, such steps as are specified in the Enforcement Notice;
- (b) refrain from taking, after such time as may be so specified, such steps as are so specified in the Enforcement Notice; or
- (c) 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 in the Enforcement Notice.

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

(3) An Enforcement Notice shall contain—

- (a) the provision of the Act that is contravened with particulars of the offence; and
- (b) particulars of the right of appeal conferred by section 89.

(4) Subject to sub-sections (5) and (6), an Enforcement Notice shall not require any of the provisions of the Enforcement Notice to be complied with before the end of the period within which an appeal can be brought against the notice and, where such an appeal is brought, the notice need

not be complied with pending the determination or withdrawal of the appeal.

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

(6) Where sub-section (5) applies, the notice shall not require the provisions of the Enforcement 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 or  
variation of an  
Enforcement  
Notice.

**75.**—(1) Where the Commissioner considers that all or any of the provisions of an Enforcement Notice need not be complied with in order to ensure compliance with this Act, he may cancel or vary the enforcement notice by written notice to the person on whom it was served.

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

Request for  
assessment.

**76.**—(1) A request may be made to the Commissioner by or on behalf of any person who is, or believes himself to be, directly affected by any processing of personal data, for an assessment as to whether processing is in compliance with this Act.

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

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

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

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

(a) the extent to which the request appears to him to raise a matter of substance;

(b) any undue delay in making the request; and

- (c) whether or not the person making the request has a right to access the personal data in question as specified in section 11.

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

- (a) whether he has made an assessment as a result of the request; and
- (b) to the extent that he considers appropriate, having regard in particular to any exemption from section 11 applying in relation to the personal data concerned, of any view formed or action taken as a result of the request.

**77.—(1)** Where the Commissioner—

Information  
notice.

- (a) has received a request under section 76 in respect of any processing of personal data; or
- (b) reasonably requires any information for the purpose of determining whether a data controller has complied or is complying with the data protection principles,

he may serve the data controller with an Information Notice, requiring the data controller to furnish him with specified information relating to the request or to compliance with the provisions of this Act.

(2) An Information Notice shall contain—

- (a) in a case falling within—
  - (i) sub-section (1)(a), a statement that the Commissioner has received a request under section 76 in relation to the specified processing; or
  - (ii) sub-section (1)(b), a statement that the Commissioner regards the specified information as relevant for the purpose of determining whether the data controller or the data processor has complied or is complying with the provisions of this Act and his reasons for regarding it as relevant for that purpose; and

(b) particulars of the right of appeal conferred by section 89.

(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 sub-section (5) and (6), a period specified in an Information Notice under sub-section (3)(b) shall not end, and a time so specified shall not fall, before the end of the period within which an appeal can be brought against the Information Notice and, where such an appeal is brought, the information shall not be furnished pending the determination or withdrawal of the appeal.

(5) Where by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, he may include in the Information Notice a statement to that effect and a statement of his reasons for reaching that conclusion and in that event sub-section (4) shall not apply, but the Information 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 a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act; or
- (b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act, including proceedings before the Tribunal, and for the purposes of such proceedings.

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

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

(9) Any relevant statement provided by a person in response to a requirement under this section may not be used in evidence against that person on a prosecution for an offence under this Act, other than an offence under section 84, unless in the proceedings—



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

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

(11) This section has effect subject to section 76(3).

(12) In sub-section (1), "specified information" means information—

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

(13) In subsection (9), "relevant statement", in relation to a requirement under this section, means—

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

**78.—(1)** Where the Commissioner—

- (a) receives a request under section 76 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(3), 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,

Special  
information  
notice

he may serve the data controller with a Special Information Notice requiring the data controller to furnish him with specified information for the purpose specified in sub-section (2).

(2) The purpose referred to in sub-section (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 appeal conferred by section 89; and
- (b) in a case falling within—
  - (i) sub-section (1)(a), a statement that the Commissioner has received a request under section 76 in relation to the specified processing; or
  - (ii) sub-section (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 a 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 sub-section (6), a period specified in a Special Information Notice under sub-section (4)(b) shall not end, and a time so specified shall not fall, before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(6) Where by reason of special circumstances the Commissioner considers that the information is required as a matter of urgency, he may include in the Special Information Notice a statement to that effect and a statement of his reasons for reaching that conclusion and in that event subsection (5) shall not apply, but the Special Information 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 a professional legal adviser and his client in connection with the giving of legal advice to the client with respect to his obligations, liabilities or rights under this Act; or
- (b) any communication between a professional legal adviser and his client, or between such an adviser or his client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act, including proceedings before the Tribunal, and for the purposes of such proceedings.

(8) In sub-section (7) a reference to the client of a professional legal adviser includes a reference to any person representing such a client.

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

(10) Any relevant statement provided by a person in response to a requirement under this section may not be used in evidence against that person on a prosecution for any offence under this Act, other than an offence under section 77, unless in the proceedings—

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

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

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

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

(13) In sub-section (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.

**79.**—(1) Where at any time it appears to the Commissioner, whether as a result of the service of a Special Information Notice or otherwise, that any personal data is not being processed—

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

he may make a determination in writing to that effect.

(2) A notice under sub-section (1) shall be given to the data controller, and shall contain particulars of the right of appeal conferred by section 89.

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

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

**80.**—(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 74(1) with respect to that data has taken effect; and
- (b) the Supreme Court has granted leave for the Enforcement Notice to be served.

(2) The Supreme Court shall not grant leave for the purposes of sub-section (1)(b) unless 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 77(1) with respect to that data has taken effect.

**81.**—(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 five thousand dollars.

Failure to  
comply with  
notice

(2) A person who, in purported compliance with an Information Notice—

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

is guilty of an offence and is liable on summary conviction to a fine of twenty thousand dollars.

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

**82.**—(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—

Service of notice  
by  
Commissioner.

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

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

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

Warrants

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

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

the Judge may issue a warrant.

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

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

(3) A Judge shall not issue a warrant in respect of any personal data processed for the purposes of journalism or for artistic or literary purposes

unless a determination by the Commissioner under section 79 with respect to those data has taken effect.

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

Execution of warrants.

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

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

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

**85.**—(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 31, is exempt from any of the provisions of this Act.

Matters exempt from inspection and seizure.

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

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

**86.** A warrant shall be returned to the Supreme Court—

Return of warrants.

- (a) after being executed; or
- (b) where not executed within the time authorised for its execution;

and the police officer by whom any such warrant is executed shall make an endorsement on it stating what powers have been exercised by him under the warrant.

## *Data Protection*

---

Obstruction of execution of a warrant.

**87.** Any person who—

- (a) intentionally obstructs a person in the execution of a warrant;
- (b) fails without reasonable excuse to give any police officer executing such a warrant such assistance as he may reasonably require for the execution of the warrant;
- (c) makes a statement in response to a requirement under section 83(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 83(2)(e) which is false in a material respect,

commits an offence and is liable on summary conviction to a fine of twenty thousand dollars.

## PART X

### *Data Protection Tribunal*

**88.—(1)** There is established a tribunal called the Data Protection Tribunal.

Establishment of the Data Protection Tribunal.

(2) The constitution of the Tribunal and other matters relating to the Tribunal shall be prescribed by the Minister by Order published in the *Gazette*.

Right of appeal.

**89.—(1)** A person on whom an Enforcement Notice, an Information Notice or a Special Information Notice has been served may appeal to the Tribunal against the notice.

(2) A person on whom an Enforcement Notice has been served may appeal to the Tribunal against the refusal of an application under 75(2) for cancellation or variation of the notice.

(3) Where an Enforcement Notice, an Information Notice or a Special Information Notice contains a statement by the Commissioner in accordance with sections 74(3), 77(5) or 78(6) then, whether or not the person appeals against the notice, he may appeal against—

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



(4) A data controller in respect of whom a determination has been made under section 90 may appeal to the Tribunal against the determination.

(5) A person on whom an order has been made pursuant to section 90 may appeal to the Tribunal against that order.

(6) A person who is aggrieved by a decision of the Commissioner may appeal to the Tribunal against that decision.

**90.**—(1) Where on an appeal under section 89(1) the Tribunal considers—

Determination of appeals.

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

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

(2) Upon appeal pursuant to subsection (1), the Tribunal may review any determination of fact on which the notice in question was based.

(3) Where on an appeal under section 89(2) the Tribunal considers that the Enforcement Notice ought to be cancelled or varied by reason of a change in circumstances, the Tribunal shall cancel or vary the notice.

(4) On an appeal under section 89(3) the Tribunal may direct—

- (a) that the notice in question shall have effect as if it did not contain any such statement as is mentioned in that subsection; or
- (b) that the inclusion of the statement in accordance with sections 74(3), 77(5) or 78(6) shall not have effect in relation to any part of the notice, and may make such modifications in the notice as may be required for giving effect to the direction.

(5) On an appeal under section 89(4), the Tribunal may cancel the determination of the Commissioner.

(6) Any party to an appeal to the Tribunal under section 89 may appeal from the decision of the Tribunal on a point of law to the Supreme Court.

(7) Any appeal under this Act may be brought within 60 days of a decision given under this Act.

## PART XI

### *Miscellaneous*

Right to  
compensation  
and liability.

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

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

Unlawful  
obtaining of  
personal data.

**92.**—(1) A person shall not knowingly or recklessly, without the consent of a 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) Sub-section (1) shall not apply to a person who shows that—

- (a) the obtaining, disclosing or procuring—
  - (i) was necessary for the purpose of preventing or detecting crime; or
  - (ii) was required or authorised by or under any enactment, by any rule of law or by the order of a court of competent jurisdiction;
- (b) he acted in the reasonable belief that he had in law, the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person;
- (c) he acted in the reasonable belief that he would have had the consent of the data controller, if, the data controller had known of the obtaining, disclosing or procuring and the circumstances of it; or

## *Data Protection*

---

(d) in the particular circumstances, the obtaining, disclosing or procuring was justified as being in the public interest.

(3) A person who, contravenes sub-section (1), commits an offence and is liable on summary conviction to a fine of ten thousand dollars.

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

Disclosure of information

**94.** The Minister may by Order published in the *Gazette* amend the Schedule.

Amendment of Schedule.

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

Regulations.

**96.** –(1) This Act comes into force on a day to be appointed by the Minister by Order published in the *Gazette*.

Commencement.

(2) Different days may be appointed for bringing different provisions into force, or for bringing different purposes of the same provision into force.

### SCHEDULE [section 81(2)]