

No. S 1

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

**CONSTITUTION OF BRUNEI DARUSSALAM
(Order made under Article 83(3))**

PERSONAL DATA PROTECTION ORDER, 2025

ARRANGEMENT OF SECTIONS

Section

PART 1

PRELIMINARY

1. Citation, commencement and long title
2. Interpretation
3. Application of Order

PART 2

ADMINISTRATION

4. Administration of this Order
5. Functions and duties of Authority
6. Advisory committees

PART 3

ACCOUNTABILITY FOR PERSONAL DATA

7. Responsibilities of organisation

PART 4

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

Division 1

Consent

8. Consent required
9. Consent to send direct marketing messages to Brunei Darussalam telephone number
10. Valid consent
11. Deemed consent
12. Deemed consent by notification
13. Withdrawal of consent
14. Collection, use and disclosure without consent

Division 2

Purpose

15. Limitation of purpose and extent
16. Personal data collected before commencement of Order
17. Notification of purpose

PART 5

RIGHTS OF INDIVIDUALS

18. Access to personal data
19. Correction of personal data
20. Exercise of rights on behalf of individual

PART 6

CARE OF PERSONAL DATA

21. Accuracy of personal data
22. Protection of personal data
23. Retention of personal data
24. Transfer of personal data outside Brunei Darussalam

PART 7

NOTIFICATION OF DATA BREACHES

25. Interpretation of this Part
26. Notifiable data breaches
27. Duty to conduct assessment of data breach
28. Duty to notify occurrence of notifiable data breach
29. Obligations of data processor of public agency

PART 8

**OFFENCES AFFECTING PERSONAL DATA AND
ANONYMISED INFORMATION**

30. Interpretation of this Part
31. Unauthorised disclosure of personal data
32. Improper use of personal data
33. Unauthorised re-identification of anonymised information

PART 9

ENFORCEMENT

34. Alternative dispute resolution
35. Power to review

- 36. Directions for non-compliance
- 37. Financial penalties
- 38. Procedure for giving of directions and imposing of financial penalty
- 39. Voluntary undertakings
- 40. Reconsideration of directions or decisions

PART 10

APPEALS

- 41. Data Protection Appeal Panel and Data Protection Appeal Committee
- 42. Appeal from direction or decision of Authority

PART 11

INVESTIGATION AND OFFENCES

- 43. Powers of investigation
- 44. Power to require documents or information
- 45. Power to require provision of information etc.
- 46. Power to enter premises without warrant
- 47. Power to enter premises under warrant
- 48. Offences and penalties
- 49. General penalty
- 50. Offences by body corporate etc.
- 51. Liability of employers for acts of employees
- 52. Composition of offences

PART 12

GENERAL

- 53. Conduct of proceedings

54. Cooperation agreements
55. Advisory guidelines
56. Certificate as to national interest
57. Evidence in proceedings
58. Enforcement of directions or decisions in High Court
59. Right of private action
60. Preservation of secrecy
61. Protection from personal liability
62. Public servants
63. Exemption
64. Amendment of Schedules
65. Regulations

SCHEDULE 1 — COLLECTION, USE AND DISCLOSURE OF
PERSONAL DATA WITHOUT CONSENT

SCHEDULE 2 — ADDITIONAL BASES FOR COLLECTION, USE AND
DISCLOSURE OF PERSONAL DATA WITHOUT
CONSENT

SCHEDULE 3 — EXCEPTIONS FROM ACCESS REQUIREMENT

SCHEDULE 4 — EXCEPTIONS FROM CORRECTION
REQUIREMENT

SCHEDULE 5 — SPECIFIED PURPOSES

SCHEDULE 6 — CONSTITUTION AND PROCEEDINGS OF APPEAL
PANEL AND APPEAL COMMITTEE

CONSTITUTION OF BRUNEI DARUSSALAM
(Order made under Article 83(3))

PERSONAL DATA PROTECTION ORDER, 2025

In exercise of the power conferred by Article 83(3) of the Constitution of Brunei Darussalam, His Majesty the Sultan and Yang Di-Pertuan hereby makes the following Order —

PART 1

PRELIMINARY

Citation, commencement and long title

1. (1) This Order may be cited as the Personal Data Protection Order, 2025 and shall commence on a date to be appointed by the Minister, with the consent of His Majesty the Sultan and Yang Di-Pertuan, by notification published in the *Gazette*.

(2) Different dates may be appointed under subsection (1) for provisions of this Order or for different purposes of the same provisions.

(3) The long title of this Order is "An Order to govern the collection, use and disclosure of personal data by organisations and for matters connected therewith".

Interpretation

2. In this Order, unless the context otherwise requires —

"advisory committee" means an advisory committee appointed under section 6;

"Appeal Committee" means the Data Protection Appeal Committee constituted under section 41(2);

"Appeal Panel" means the Data Protection Appeal Panel established by section 41(1);

"authorised officer" means any person appointed as an authorised officer under section 4(2);

"Authority" means the Authority for Info-communications Technology Industry of Brunei Darussalam established by section 3 of the Authority for Info-communications Technology Industry of Brunei Darussalam Order, 2001 (S 39/2001);

"business" includes the activity of any organisation, whether or not carried on for purposes of gain, or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in his personal or domestic capacity;

"business contact information" means an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes;

"credit bureau" means an organisation which –

(a) provides credit reports for gain or profit; or

(b) provides credit reports on a routine, non-profit basis as an ancillary part of a business carried on for gain or profit;

"credit report" means a communication, whether in written, oral or other form, provided to an organisation to assess the creditworthiness of an individual in relation to a transaction between the organisation and the individual;

"data processor" means an organisation which processes personal data on behalf of another organisation or public agency;

"direct marketing message" means a message, whether in sound, text, visual or other form, containing advertising or marketing material of a commercial nature which is directed to a particular individual;

"education institution" means any organisation that provides education, including instruction, training or teaching, whether by itself or in association or collaboration with or by affiliation with any other person;

"employee" has the same meaning assigned to it under the Employment Order, 2009 (S 37/2009) and includes a volunteer;

"employment" includes working under an unpaid volunteer work relationship;

"evaluative purpose" means —

(a) for the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates —

- (i) for employment or for appointment to office;
- (ii) for promotion in employment or office or for continuance in employment or office;
- (iii) for removal from employment or office;
- (iv) for admission to an education institution;
- (v) for the awarding of contracts, awards, bursaries, scholarships, honours or other similar benefits;
- (vi) for selection for an athletic or artistic purpose; or
- (vii) for grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency;

(b) for the purpose of determining whether any contract, award, bursary, scholarship, honour or other similar benefit should be continued, modified or cancelled;

(c) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property; or

(d) for such other similar purposes as the Authority may determine;

"individual" means a natural person, whether living or deceased;

"investigation" means an investigation relating to —

(a) a breach of an agreement;

(b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(c) a circumstance or conduct that may result in a remedy or relief being available under any written law;

"Minister" means the Minister responsible for personal data protection;

"national interest" includes national defence, national security, public security, the maintenance of essential services and the conduct of international affairs;

"organisation" includes any individual, company, association or body of persons, corporate or unincorporated, whether or not —

(a) formed or recognised under the law of Brunei Darussalam; or

(b) resident, or having an office or a place of business, in Brunei Darussalam;

"personal data" means data, whether true or not, about an individual who can be identified —

(a) from that data; or

(b) from that data and other information to which the organisation has or is likely to have access;

"prescribed healthcare body", for the purposes of Schedule 2, means a healthcare body declared by the Minister of Health, by notification published in the *Gazette*;

"prescribed law enforcement agency", for the purposes of sections 18(4) and 28(6)(a) and Schedule 2, means a relevant authority charged with the duty of investigating offences or charging offenders under any written law, declared by the relevant Minister responsible for that authority, by notification published in the *Gazette*;

"private trust" means a trust for the benefit of one or more designated individuals who are friends, or members of the family, of the settlor;

"proceedings" means any civil, criminal or administrative proceedings by or before a court, tribunal or regulatory authority that is related to the allegation of —

(a) a breach of an agreement;

(b) a contravention of any written law or any rule of professional conduct or other requirement imposed by any regulatory authority in exercise of its powers under any written law; or

(c) a wrong or a breach of a duty for which a remedy is claimed under any law;

"processing", in relation to personal data, means the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following —

(a) collection;

(b) recording;

(c) holding or storage;

(d) organisation, structuring, adaptation or alteration;

(e) retrieval;

(f) alignment or combination;

(g) use;

(h) disclosure by transmission, dissemination or otherwise making available;

(i) erasure or destruction;

"public agency" includes —

(a) the Government, including any ministry, department, agency, or organ of State;

(b) any tribunal appointed under any written law; or

(c) any statutory body as the Minister may, by notification published in the *Gazette*, specify to be a public agency for the purposes of this Order;

"publicly available", in relation to personal data about an individual, means personal data that is generally available to the public, and includes personal

data which can be observed by reasonably expected means at a location or an event —

(a) at which the individual appears; and

(b) that is open to the public.

Application of Order

3. (1) Parts 3, 4, 5, 6 and 7 do not impose any obligation on —

(a) any individual acting in a personal or domestic capacity;

(b) any employee acting in the course of his employment with an organisation;

(c) any public agency; or

(d) any other organisations or personal data, or classes of organisations or personal data, prescribed for the purposes of this provision.

(2) Parts 3, 4, 5, 6 (except sections 22, 23 and 24) and 7 (except sections 27(2)(a) and 29) do not impose any obligation on a data processor in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

(3) An organisation has the same obligation under this Order in respect of personal data processed on its behalf and for its purposes by a data processor as if the personal data were processed by the organisation itself.

(4) This Order does not apply in respect of —

(a) personal data about an individual that is contained in a record that has been in existence for at least 100 years; or

(b) personal data about a deceased individual, except that the provisions relating to the disclosure and protection of personal data apply in respect of personal data about an individual who has been dead for 10 years or fewer.

(5) Except where business contact information is expressly referred to, Parts 3, 4, 5, 6 and 7 do not apply to business contact information.

(6) Unless otherwise expressly provided in this Order —

(a) nothing in Parts 3, 4, 5, 6 and 7 affects any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation is not an excuse for contravening this Order; and

(b) the provisions of any other written law prevail to the extent that any provision of Parts 3, 4, 5, 6 and 7 is inconsistent with the provisions of that other written law.

PART 2

ADMINISTRATION

Administration of this Order

4. (1) The Authority is responsible for the administration of this Order.

(2) The Authority may appoint such number of authorised officers to carry into effect any specific provision of this Order or of any regulations made thereunder.

Functions and duties of Authority

5. (1) It shall be the function and duty of the Authority —

(a) to promote awareness of data protection in Brunei Darussalam;

(b) to provide consultancy, advisory, training, technical, managerial or other specialist services relating to data protection;

(c) to advise the Government on national needs and policies on matters relating to data protection;

(d) to act internationally as the national body representative of Brunei Darussalam on matters relating to data protection;

(e) to conduct research and studies and promote educational activities relating to data protection, including organising and conducting seminars, workshops and symposia relating thereto, and supporting other organisations conducting such activities;

(f) to manage technical cooperation and exchange in the area of data protection with other organisations, including foreign data protection authorities and international or intergovernmental organisations, on its own behalf or on behalf of the Government;

(g) to administer and enforce this Order; and

(h) to carry out functions conferred on the Authority under any other written law.

(2) Nothing in this section is construed as imposing on the Authority, directly or indirectly, any form of duty or liability enforceable by proceedings before any court.

Advisory committees

6. (1) The Minister may appoint one or more advisory committees to provide advice to the Authority with regard to the performance of any of its functions under this Order.

(2) The Authority may consult such advisory committees in relation to the performance of its functions and duties and the exercise of its powers under this Order but is not bound by the consultation.

PART 3

ACCOUNTABILITY FOR PERSONAL DATA

Responsibilities of organisation

7. (1) In meeting its responsibilities under this Order, an organisation —

(a) shall consider what a reasonable person would consider appropriate in the circumstances including, without limitation, —

(i) the nature, scope and context of, and purposes for, the organisation's collection, use or disclosure of personal data; and

(ii) the nature, type and amount of personal data which may be collected, used or disclosed by the organisation;

(b) is responsible for personal data in its possession or under its control;

(c) shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Order;

(d) shall make available to the public the business contact information of at least one of the individuals designated under paragraph (c);

(e) shall —

- (i) develop and implement policies and practices that are necessary for the organisation to meet the obligations of the organisation under this Order;
- (ii) develop a process to receive and respond to complaints that may arise with respect to the application of this Order;
- (iii) communicate to its staff information about the organisation's policies and practices referred to in sub-paragraph (i); and
- (iv) make information available on request about —
 - (A) the policies and practices referred to in sub-paragraph (i);
 - (B) the complaint process referred to in sub-paragraph (ii).

(2) Without limiting subsection (1)(d), an organisation is deemed to have satisfied subsection (1)(d) if the organisation makes available the business contact information of any individual mentioned in subsection (1)(c) in any prescribed manner.

(3) The designation of an individual by an organisation under subsection (1)(c) does not relieve the organisation of any of its obligations under this Order.

PART 4

COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

Division 1

Consent

Consent required

8. No organisation shall collect, use or disclose personal data about an individual unless —

(a) the individual gives, or is deemed to have given, his consent under this Order to the collection, use or disclosure; or

(b) the collection, use or disclosure without the consent of the individual is required or authorised under this Order or any other written law.

Consent to send direct marketing messages to Brunei Darussalam telephone number

9. Notwithstanding section 8, no organisation shall use a Brunei Darussalam telephone number of an individual to send a direct marketing message to the individual unless —

(a) the individual gives his clear and unambiguous consent under this Order to use his Brunei Darussalam telephone number to send a direct marketing message; or

(b) the use of the individual's Brunei Darussalam telephone number to send a direct marketing message without the consent of the individual is required or authorised under this Order or any other written law.

Valid consent

10. (1) An individual has not given consent under this Order for the collection, use or disclosure of personal data about the individual by an organisation for a purpose unless —

(a) the individual has been provided with the information required under section 17; and

(b) the individual provided his consent for that purpose in accordance with this Order.

(2) An individual has not given clear and unambiguous consent under this Order for the use of his Brunei Darussalam telephone number for the purpose of receiving a direct marketing message unless —

(a) the individual has been provided with the information required under section 17;

(b) the individual provided his consent for that purpose in accordance with this Order; and

(c) the consent of the individual is given in written or other form so as to be accessible for subsequent reference.

(3) No organisation shall —

(a) as a condition of providing a product or service, require an individual to consent to the collection, use or disclosure of personal data about the individual beyond what is reasonable to provide the product or service to that individual; or

(b) obtain or attempt to obtain consent for collecting, using or disclosing personal data by providing false or misleading information with respect to the collection, use or disclosure of the personal data, or using deceptive or misleading practices.

(4) Any consent given in any of the circumstances in subsection (3) is not validly given for the purposes of this Order.

Deemed consent

11. (1) An individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation for a purpose if —

(a) the individual, without actually giving consent referred to in section 10, voluntarily provides the personal data to the organisation for that purpose; and

(b) it is reasonable that the individual would voluntarily provide the data.

(2) If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation.

(3) Without limiting subsection (2) and subject to subsection (7), an individual (*P*) who provides personal data to an organisation (*A*) with a view to *P* entering into a contract with *A* is deemed to consent to the following —

(a) the disclosure of that personal data by *A* to another organisation (*B*), where the disclosure is reasonably necessary for the conclusion of the contract between *P* and *A*;

(b) the collection and use of that personal data by *B*, where the collection and use is reasonably necessary for the conclusion of the contract between *P* and *A*;

(c) the disclosure of that personal data by *B* to another organisation, where the disclosure is reasonably necessary for the conclusion of the contract between *P* and *A*.

(4) Where an organisation collects personal data disclosed to it by *B* under subsection (3)(c), subsection (3)(b) and (c) applies to the organisation as if the personal data were disclosed by *A* to the organisation under subsection (3)(a).

(5) Without limiting subsection (2) and subject to subsection (7), an individual (*P*) who enters into a contract with an organisation (*A*) and provides personal data to *A* pursuant or in relation to that contract is deemed to consent to the following –

(a) the disclosure of that personal data by *A* to another organisation (*B*), where the disclosure is reasonably necessary –

- (i) for the performance of the contract between *P* and *A*; or
- (ii) for the conclusion or performance of a contract between *A* and *B* which is entered into at *P*'s request, or if a reasonable person would consider the contract to be in *P*'s interest;

(b) the collection and use of that personal data by *B*, where the collection and use are reasonably necessary for any purpose mentioned in paragraph (a);

(c) the disclosure of that personal data by *B* to another organisation, where the disclosure is reasonably necessary for any purpose mentioned in paragraph (a).

(6) Where an organisation collects personal data disclosed to it by *B* under subsection (5)(c), subsection (5)(b) and (c) applies to the organisation as if the personal data were disclosed by *A* to the organisation under subsection (5)(a).

(7) Subsections (3), (4), (5) and (6) do not affect any obligation under the contract between *P* and *A* that specifies or restricts –

(a) the personal data provided by *P* that *A* may disclose to another organisation; or

(b) the purposes for which *A* may disclose the personal data provided by *P* to another organisation.

Deemed consent by notification

12. (1) Subject to subsection (2), an individual is deemed to consent to the collection, use or disclosure of personal data about the individual by an organisation if –

(a) the organisation satisfies the requirements in subsection (3); and

(b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (3)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation.

(2) Subsection (1) does not apply to the collection, use or disclosure of personal data about the individual for the purpose of sending a direct marketing message.

(3) For the purposes of subsection (1)(a), the organisation shall, before collecting, using or disclosing any personal data about the individual –

(a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual; and

(b) take reasonable steps to bring the following information to the attention of the individual –

- (i) the organisation's intention to collect, use or disclose the personal data;
- (ii) the purpose for which the personal data will be collected, used or disclosed;
- (iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data.

(4) The organisation shall, in respect of the assessment mentioned in subsection (3)(a) —

(a) identify any adverse effect that the proposed collection, use or disclosure of the personal data for the relevant purpose is likely to have on the individual;

(b) identify and implement reasonable measures —

(i) to eliminate the adverse effect;

(ii) to reduce the likelihood that the adverse effect will occur; or

(iii) to mitigate the adverse effect; and

(c) comply with any other prescribed requirements.

Withdrawal of consent

13. (1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Order, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose.

(2) On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of the likely consequences of withdrawing his consent.

(3) No organisation shall prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section does not affect any legal consequences arising from such withdrawal.

(4) Subject to section 23, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data processors and agents to cease) collecting, using or disclosing the personal data, unless such collection, use or disclosure without the consent of the individual is required or authorised under this Order or any other written law.

Collection, use and disclosure without consent

14. (1) An organisation may —

(a) collect personal data about an individual, without the consent of the individual or from a source other than the individual, in the

circumstances or for the purposes, and subject to any condition, in Schedule 1 or Part 1 of Schedule 2;

(b) use personal data about an individual without the consent of the individual, in the circumstances or for the purposes, and subject to any condition, in Schedule 1 or Part 2 of Schedule 2; or

(c) disclose personal data about an individual without the consent of the individual, in the circumstances or for the purposes, and subject to any condition, in Schedule 1 or Part 3 of Schedule 2.

(2) Unless otherwise provided under this Order, an organisation may —

(a) collect personal data about an individual that is disclosed to the organisation in accordance with subsection (1)(c) for purposes consistent with the purpose of that disclosure; or

(b) use or disclose personal data about an individual that is collected by the organisation in accordance with subsection (1)(a) for purposes consistent with the purpose of that collection.

Division 2

Purpose

Limitation of purpose and extent

15. An organisation may collect, use or disclose personal data about an individual —

(a) only for purposes that a reasonable person would consider appropriate in the circumstances; and

(b) that are relevant and limited to what are reasonably necessary for its purposes.

Personal data collected before commencement of Order

16. (1) Notwithstanding the other provisions in this Part, an organisation may use personal data about an individual collected before the date of commencement of this Order for the purposes for which the personal data was collected unless —

(a) consent for such use is withdrawn in accordance with section 13; or

(b) the individual, whether before, on or after the date of commencement of this Order, has otherwise indicated to the organisation that he opts-out or otherwise does not consent to the use of the personal data.

(2) No organisation shall use a Brunei Darussalam telephone number of the individual for the purpose of sending a direct marketing message unless the organisation has given the individual a reasonable opportunity to opt-out from receiving the direct marketing message.

Notification of purpose

17. (1) An organisation may collect, use or disclose personal data about an individual only for purposes that the individual has been informed of under subsection (2), if applicable.

(2) For the purposes of section 10(1)(a) and subsection (1), an organisation shall inform the individual of –

(a) the purposes for the collection, use or disclosure of the personal data on or before collecting the personal data;

(b) any other purpose of the use or disclosure of the personal data of which the individual has not been informed under paragraph *(a)*, before the use or disclosure of the personal data for that purpose; and

(c) on request by the individual, the business contact information of a person who is able to answer on behalf of the organisation the individual's questions about the collection, use or disclosure of the personal data.

(3) An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Order.

(4) Subsection (2) does not apply if –

(a) the individual is deemed to have consented to the collection, use or disclosure under section 11 or 12; or

(b) the organisation collects, uses or discloses the personal data without the consent of the individual in accordance with section 14.

(5) Notwithstanding subsection (4), an organisation shall comply with subsection (6) on or before collecting, using or disclosing personal data about an individual for the purpose of or in relation to the organisation —

(a) entering into an employment relationship with the individual or appointing the individual to any office; or

(b) managing or terminating the employment relationship with or appointment of the individual.

(6) For the purposes of subsection (5), the organisation shall inform the individual of the following —

(a) the purpose for which the organisation is collecting, using or disclosing the personal data about the individual;

(b) on request by the individual, the business contact information of a person who is able to answer the individual's questions about that collection, use or disclosure on behalf of the organisation.

PART 5

RIGHTS OF INDIVIDUALS

Access to personal data

18. (1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with —

(a) personal data about the individual that is in the possession or under the control of the organisation; and

(b) information about the ways in which the personal data referred to in paragraph *(a)* has been or may have been used or disclosed by the organisation within a year before the date of the request.

(2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in Schedule 3.

(3) No organisation shall provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information could reasonably be expected to —

(a) threaten the safety or physical or mental health of an individual other than the individual who made the request;

(b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;

(c) reveal personal data about another individual;

(d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or

(e) be contrary to the national interest.

(4) No organisation shall inform any individual under subsection (1)/*(b)* that the organisation has disclosed personal data about the individual to a prescribed law enforcement agency if the disclosure was made without the consent of the individual under this Order or any other written law.

(5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4).

(6) Where, by reason of subsection (2) or (3), an organisation refuses to or otherwise does not provide an individual with the individual's personal data or other information requested under subsection (1), the organisation shall —

(a) notify the individual of the refusal within the prescribed time and in accordance with the prescribed requirements; and

(b) preserve, for not less than the prescribed period, a copy of the personal data concerned, if available.

(7) Where an organisation provides an individual, in accordance with subsection (5), with the individual's personal data or other information requested under subsection (1), the organisation shall notify the individual of the exclusion of any personal data or other information so requested under subsection (2) or (3).

(8) The organisation shall ensure that the copy of the personal data it preserves for the purposes of subsection (6)/*(b)* is a complete and accurate copy of the personal data concerned.

Correction of personal data

19. (1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation.

(2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall —

(a) correct the personal data as soon as practicable; and

(b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

(3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date the correction was made.

(4) When an organisation is notified under subsection (2)(b) or (3) of a correction of personal data, the organisation shall correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made.

(5) If no correction is made under subsection (2)(a) or (4), the organisation shall annotate the personal data in its possession or under its control with the correction that was requested but not made.

(6) Nothing in this section shall require an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion.

(7) An organisation is not required to comply with this section in respect of the matters specified in Schedule 4.

Exercise of rights on behalf of individual

20. Any person validly acting on behalf of an individual in relation to the exercise of the individual's rights under this Order may —

(a) give, or be deemed to have given, any consent for the collection, use or disclosure of the individual's personal data under this Order;

(b) withdraw any consent given, or deemed to have been given, for the collection, use or disclosure of the individual's personal data under this Order;

(c) make any request for access to the individual's personal data under section 18; or

(d) make any request for correction of the individual's personal data under section 19; or

(e) make such other request or take such other action as may be prescribed in relation to the individual's personal data.

PART 6

CARE OF PERSONAL DATA

Accuracy of personal data

21. An organisation shall make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data —

(a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or

(b) is likely to be disclosed by the organisation to another organisation.

Protection of personal data

22. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent —

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

Retention of personal data

23. An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that —

(a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and

(b) retention is no longer necessary for legal or business purposes.

Transfer of personal data outside Brunei Darussalam

24. (1) No organisation shall transfer any personal data to a country outside Brunei Darussalam except in accordance with the prescribed requirements to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under this Order.

(2) The Authority may, on the application of any organisation, by notice in writing exempt the organisation from any prescribed requirement pursuant to subsection (1) in respect of any transfer of personal data by that organisation.

(3) An exemption under subsection (2) —

(a) may be granted subject to such conditions as the Authority may specify in writing; and

(b) need not be published in the *Gazette* and may be revoked at any time by the Authority.

(4) The Authority may at any time add to, vary or revoke any condition imposed under this section.

PART 7

NOTIFICATION OF DATA BREACHES

Interpretation of this Part

25. In this Part, unless the context otherwise requires —

"affected individual" means any individual to whom any personal data affected by a data breach relates;

"data breach", in relation to personal data, means —

(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or

(b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

Notifiable data breaches

26. (1) A data breach is a notifiable data breach if the data breach —

(a) results in, or is likely to result in, significant harm to an affected individual; or

(b) is, or is likely to be, of a significant scale.

(2) Without limiting subsection (1)*(a)*, a data breach is deemed to result in significant harm to an individual —

(a) if the data breach is in relation to any prescribed personal data or class of personal data relating to the individual; or

(b) in other prescribed circumstances.

(3) Without limiting subsection (1)*(b)*, a data breach is deemed to be of a significant scale —

(a) if the data breach affects not fewer than the prescribed number of affected individuals; or

(b) in other prescribed circumstances.

(4) Notwithstanding subsections (1), (2) and (3), a data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data only within an organisation is deemed not to be a notifiable data breach.

Duty to conduct assessment of data breach

27. (1) Subject to subsection (2), where an organisation has reason to believe that a data breach affecting personal data in its possession or under its control has occurred, the organisation shall conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.

(2) Where a data processor (other than a data processor mentioned in section 29) has reason to believe that a data breach has occurred in relation to personal data that the data processor is processing on behalf of and for the purposes of another organisation —

(a) the data processor shall, without undue delay, notify the other organisation of the occurrence of the data breach; and

(b) the other organisation shall, on notification by the data processor, conduct an assessment of whether the data breach is a notifiable data breach.

(3) The organisation shall carry out the assessment mentioned in subsection (1) or 2(b) in accordance with any prescribed requirements.

Duty to notify occurrence of notifiable data breach

28. (1) Where an organisation assesses, in accordance with section 27, that a data breach is a notifiable data breach, the organisation shall notify the Authority as soon as is practicable, but in any case no later than 3 days after the day the organisation makes that assessment.

(2) Subject to subsections (5), (6) and (7), on or after notifying the Authority under subsection (1), the organisation shall also notify each affected individual affected by a notifiable data breach mentioned in section 26(1)(a) in any manner that is reasonable in the circumstances.

(3) The notification under subsection (1) or (2) shall contain, to the best of the knowledge and belief of the organisation at the time it notifies the Authority or affected individual, all the information that is prescribed for this purpose.

(4) The notification under subsection (1) shall be made in such form and manner as the Authority may require.

(5) Subsection (2) does not apply to an organisation in relation to an affected individual if the organisation –

(a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or

(b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

(6) No organisation shall notify any affected individual in accordance with subsection (2) if –

(a) a prescribed law enforcement agency so instructs; or

(b) the Authority so directs.

(7) The Authority may, on the written application of an organisation, waive the requirement to notify an affected individual under subsection (2) subject to any condition that the Authority thinks fit.

(8) An organisation is not, by reason only of notifying the Authority under subsection (1) or an affected individual under subsection (2), to be regarded as being in breach of –

(a) any duty or obligation under any written law or rule of law, or any contract, as to secrecy or other restriction on the disclosure of information; or

(b) any rule of professional conduct applicable to the organisation.

(9) Subsections (1) and (2) apply concurrently with any obligation of the organisation under any other written law to notify any other person (including any public agency) of the occurrence of a data breach, or to provide any information relating to a data breach.

Obligations of data processor of public agency

29. Where an organisation –

(a) is a data processor processing personal data on behalf of and for the purposes of a public agency; and

(b) has reason to believe that a data breach has occurred in relation to that personal data,

the organisation shall, without undue delay, notify the public agency of the occurrence of the data breach.

PART 8

OFFENCES AFFECTING PERSONAL DATA AND ANONYMISED INFORMATION

Interpretation of this Part

30. In this Part, unless the context otherwise requires –

“disclose”, in relation to personal data, includes providing access to personal data;

"gain" means —

(a) a gain in property or a supply of services, whether temporary or permanent; or

(b) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration;

"harm", in relation to an individual, means —

(a) any physical harm; or

(b) harassment, alarm or distress caused to the individual;

"loss" means —

(a) a loss in property or a supply of services, whether temporary or permanent; or

(b) a loss of an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration,

but does not include, in relation to an individual, the loss of personal data about the individual.

Unauthorised disclosure of personal data

31. (1) If —

(a) an individual discloses, or the individual's conduct causes disclosure of, personal data in the possession or under the control of an organisation or a public agency to another person;

(b) the disclosure is not authorised by the organisation or public agency; and

(c) the individual does so —

(i) knowing that the disclosure is not authorised by the organisation or public agency; or

(ii) reckless as to whether the disclosure is or is not authorised by the organisation or public agency,

the individual is guilty of an offence and liable on conviction to a fine not exceeding \$5,000, imprisonment for a term not exceeding 2 years or both.

(2) In proceedings for an offence under subsection (1), it is a defence to the charge for the accused to prove, on a balance of probabilities, any of the following –

(a) that –

- (i) the personal data in the possession or under the control of an organisation or a public agency, that was disclosed was, at the time of the disclosure, publicly available; and
- (ii) where the personal data was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case;

(b) that the accused disclosed, or caused the disclosure of, personal data in the possession or under the control of the organisation or public agency –

- (i) as permitted or required by or under any written law (other than this Order);
- (ii) as authorised or required by an order of court;
- (iii) in the reasonable belief that, and was not reckless as to whether, the accused had the legal right to do so; or
- (iv) in any other circumstances, or for any other purpose, prescribed.

(3) For the avoidance of doubt, subsection (2) does not affect any obligation or limitation imposed on, or prohibition of, the disclosure of personal data in the possession or under the control of an organisation or a public agency by or under any written law.

(4) In this section, "applicable contravention" means a contravention of any of the following –

- (a) subsection (1);
- (b) section 33(1).

Improper use of personal data

32. (1) If —

(a) an individual makes use of personal data in the possession or under the control of an organisation or a public agency;

(b) the use is not authorised by the organisation or public agency;

(c) the individual does so —

(i) knowing that the use is not authorised by the organisation or public agency; or

(ii) reckless as to whether the use is or is not authorised by the organisation or public agency; and

(d) the individual, as a result of that use —

(i) obtains a gain for the individual or another person;

(ii) causes harm to another individual; or

(iii) causes a loss to another person,

the individual is guilty of an offence and liable on conviction to a fine not exceeding \$5,000, imprisonment for a term not exceeding 2 years or both.

(2) In proceedings for an offence under subsection (1), it is a defence to the charge for the accused to prove, on a balance of probabilities, any of the following —

(a) that —

(i) the personal data in the possession or under the control of an organisation or a public agency that was used was, at the time of the use, publicly available; and

(ii) where the personal data was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case;

(b) the accused used the personal data in the possession or under the control of the organisation or public agency —

- (i) as permitted or required by or under any other written law (other than this Order);
- (ii) as authorised or required by an order of court;
- (iii) in the reasonable belief that, and was not reckless as to whether, the accused had the legal right to do so; or
- (iv) in any other circumstances, or for any other purpose, prescribed.

(3) For the avoidance of doubt, subsection (2) does not affect any obligation or limitation imposed on, or prohibition of, the use of personal data in the possession or under the control of an organisation or a public agency by or under any other written law.

(4) In this section, "applicable contravention" means a contravention of section 31(1) or 33(1).

Unauthorised re-identification of anonymised information

33. (1) If —

(a) an individual takes any action to re-identify or cause re-identification of the individual to whom anonymised information in the possession of or under the control of an organisation or a public agency relates (referred to in this section as the affected individual);

(b) the re-identification is not authorised by the organisation or public agency; and

(c) the individual does so —

- (i) knowing that the re-identification is not authorised by the organisation or public agency; or
- (ii) reckless as to whether the re-identification is or is not authorised by the organisation or public agency,

the individual is guilty of an offence and liable on conviction to a fine not exceeding \$5,000, imprisonment for a term not exceeding 2 years or both.

(2) In proceedings for an offence under subsection (1), it is a defence to the charge for the accused to prove, on a balance of probabilities, any of the following —

(a) that —

- (i) the information on the identity of the affected individual is publicly available; and
- (ii) where that information was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case;

(b) the action to re-identify or cause re-identification is —

- (i) permitted or required by or under any other written law (other than this Order); or
- (ii) authorised or required by an order of court;

(c) the accused —

- (i) reasonably believed that the re-identification was for a specified purpose; and
- (ii) notified the Authority or the organisation or public agency of the re-identification as soon as is practicable;

(d) the accused took the action to re-identify or cause re-identification in the reasonable belief that, and was not reckless as to whether, the accused had the legal right to do so, other than for a specified purpose;

(e) in any other circumstances, or for any other purpose, prescribed.

(3) For the avoidance of doubt, subsection (2) does not affect any obligation or limitation imposed on, or prohibition of, the re-identification of the affected individual by or under any other written law.

(4) In this section —

“applicable contravention” means a contravention of subsection (1);

“specified purpose” means any purpose specified in Schedule 5.

PART 9
ENFORCEMENT

Alternative dispute resolution

34. (1) If the Authority is of the opinion that any complaint by an individual (referred to in this section as the complainant) against an organisation may more appropriately be resolved by mediation, the Authority may, without the consent of the complainant and the organisation, refer the matter to mediation under a dispute resolution scheme.

(2) Subject to subsection (1), the Authority may, with or without the consent of the complainant and the organisation, direct the complainant or the organisation or both to attempt to resolve the complaint of the complainant in the way directed by the Authority.

(3) For the purposes of subsection (1), the Authority may establish or approve one or more dispute resolution schemes for the resolution of complaints by individuals against organisations.

Power to review

35. (1) On the application of a complainant, the Authority may review —

(a) a refusal by an organisation to provide access to personal data or other information requested by the complainant under section 18, or the organisation's failure to provide that access within a reasonable time;

(b) a refusal by an organisation to correct personal data in accordance with a request by the complainant under section 19, or the organisation's failure to make the correction within a reasonable time; or

(c) a fee required from the complainant by an organisation in relation to a request by the complainant under section 18 or 19.

(2) On completion of its review under subsection (1), the Authority may —

(a) confirm the refusal to provide access to the personal data or other information, or direct the organisation to provide access to the personal data or other information within the time specified by the Authority;

(b) confirm the refusal to correct the personal data, or direct the organisation to correct the personal data in the manner and within the time specified by the Authority; or

(c) confirm, reduce or disallow a fee, or direct the organisation to make a refund to the complainant.

Directions for non-compliance

36. (1) The Authority may, if it is satisfied that an organisation has not complied or is not complying with any provision of Part 3, 4, 5, 6 or 7, give the organisation any direction that the Authority thinks fit in the circumstances to ensure compliance with that provision.

(2) Without limiting subsection (1), the Authority may, if it thinks fit in the circumstances to ensure compliance with any provision of Part 3, 4, 5, 6 or 7, give an organisation all or any of the following directions –

(a) to stop collecting, using or disclosing personal data in contravention of this Order;

(b) to destroy personal data collected in contravention of this Order;

(c) to comply with any direction of the Authority under section 35(2).

Financial penalties

37. (1) Subject to subsection (2), the Authority may, if it is satisfied that an organisation has intentionally or negligently contravened any provision of Part 3, 4, 5, 6 or 7, require, by notice in writing, the organisation to pay a financial penalty.

(2) Subsection (1) does not apply in relation to any contravention of a provision of this Order, the breach of which is an offence under this Order.

(3) A financial penalty imposed on an organisation under subsection (1) shall not exceed the maximum amount, which in no case may be more than the following –

(a) in the case of a contravention by an organisation whose annual turnover in Brunei Darussalam exceeds \$10,000,000, 10 *per cent* of the annual turnover of the organisation in Brunei Darussalam;

(b) in any other case, \$1,000,000.

(4) The Authority shall, in determining the amount of a financial penalty imposed under subsection (1), have regard to, and give such weight as the Authority considers appropriate to, all of the following matters –

(a) the nature, gravity and duration of the non-compliance by the organisation;

(b) the type and nature of the personal data affected by the non-compliance by the organisation;

(c) whether the organisation, as a result of the non-compliance, gained any financial benefit or avoided any financial loss;

(d) whether the organisation took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action;

(e) whether the organisation had, notwithstanding the non-compliance, implemented adequate and appropriate measures for compliance with the requirements under this Order;

(f) whether the organisation had previously failed to comply with this Order;

(g) the compliance of the organisation with any direction given under section 36 or 39(4) in relation to remedying or mitigating the effect of the non-compliance;

(h) whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with this Order;

(i) the likely impact of the imposition of the financial penalty on the organisation, including the ability of the organisation to continue the usual activities of the organisation;

(j) any other matter that may be relevant.

(5) For the purposes of subsection (3)(a), the annual turnover in Brunei Darussalam of an organisation is the amount ascertained from the most recent audited accounts of the organisation available at the time the financial penalty is imposed on that organisation.

Procedure for giving of directions and imposing of financial penalty

38. (1) Before giving any direction under section 36 or imposing a financial penalty under section 37(1), the Authority shall give notice in writing to the organisation concerned —

(a) stating that the Authority intends to take action against the organisation under section 36 or 37(1);

(b) where the Authority intends to give any direction under section 36, specifying the direction the Authority proposes to give;

(c) specifying each instance of non-compliance that is the subject of the proposed action, or the reason or reasons for the proposed action; and

(d) subject to subsections (2) and (3), specifying the time within which written representations may be made to the Authority with respect to the proposed action.

(2) Where the Authority intends to impose a financial penalty under section 37(1) on an organisation, the time specified in the notice within which written representations may be made to the Authority shall be at least 14 days after the date the notice is served on that organisation.

(3) The Authority may, on written application by the organisation concerned (whether before, on or after the expiry of the time specified in the notice), extend the time for the organisation to make written representations to the Authority if the Authority is satisfied that the extension should be granted by reason of exceptional circumstances in the particular case.

(4) The Authority may decide to give the direction under section 36 or impose the financial penalty under section 37(1) —

(a) after considering any written representation made to the Authority pursuant to the notice mentioned in subsection (1); or

(b) on the expiry of the time specified in the notice under subsection (1)(d), or as extended by the Authority under subsection (3), where no representation is so made or any written representation made is subsequently withdrawn.

(5) Subsection (1) does not apply where the organisation has died, is adjudged bankrupt, has been dissolved or wound up or has otherwise ceased to exist.

(6) Where the Authority decides to give the direction under section 36 or impose the financial penalty under section 37(1), the Authority shall serve a notice of the decision on the following persons —

(a) the organisation concerned;

(b) the complainant whose complaint against the organisation concerned resulted in the giving of the direction or the imposition of the financial penalty, if any.

(7) A direction given under section 36 or the imposition of a financial penalty under section 37(1) takes effect only when the Authority serves the notice in subsection (6)(a) on the organisation concerned.

(8) Where the Authority imposes a financial penalty under section 37(1) on an organisation, the notice in writing issued by the Authority to the organisation shall specify the date before which the financial penalty is to be paid, being a date not earlier than 28 days after the notice is issued.

(9) The Authority may, on written application by an organisation on whom a financial penalty under section 37(1) is imposed —

(a) extend the time for the organisation to pay the financial penalty; or

(b) allow the financial penalty to be paid by instalments.

(10) The interest payable —

(a) on the outstanding amount of any financial penalty imposed under section 37(1); and

(b) for payment by instalments, as the Authority may allow, of any financial penalty imposed under section 37(1),

shall be at such rate as the Authority may direct, which shall not exceed the rate prescribed in the Rules of Court made under the Supreme Court Act (Chapter 5) in respect of judgment debts.

Voluntary undertakings

39. (1) Without affecting sections 36, 37(1) and 43(1), where the Authority has reasonable grounds to believe that an organisation has not complied, is not complying or is likely not to comply with any provision of Part 3, 4, 5, 6 or 7, the organisation concerned may give, and the Authority may accept, a written voluntary undertaking.

(2) Without limiting the matters to which the voluntary undertaking may relate, the voluntary undertaking may include any of the following undertakings by the organisation concerned —

(a) an undertaking to take specified action within a specified time;

(b) an undertaking to refrain from taking specified action;

(c) an undertaking to publicise the voluntary undertaking.

(3) Subject to subsection (4), the Authority may, after accepting the voluntary undertaking and with the agreement of the organisation who gave the voluntary undertaking –

(a) vary the terms of any undertaking included in the voluntary undertaking; or

(b) include, in the voluntary undertaking, any additional undertaking mentioned in subsection (2).

(4) Where an organisation fails to comply with any undertaking in a voluntary undertaking –

(a) the Authority may give the organisation concerned any direction that the Authority thinks fit in the circumstances to ensure the compliance of the organisation with that undertaking; and

(b) section 38(1), (3), (4), (5), (6) and (7) applies to the direction given under paragraph (a) as if the direction were given under section 36.

(5) In addition, where an organisation fails to comply with an undertaking mentioned in subsection (2)(c), the Authority may publicise the voluntary undertaking in accordance with the undertaking, and recover the costs and expenses so incurred from the organisation as a debt due to the Authority.

Reconsideration of directions or decisions

40. (1) An organisation or an individual aggrieved by –

(a) any direction made by the Authority under section 34(2), 36(1) or (2) or 39(4); or

(b) any direction or decision made under section 35(2),

may make a written application to the Authority to reconsider the direction or decision in accordance with this section.

(2) An organisation aggrieved by a financial penalty imposed by the Authority under section 37(1) on the organisation may make a written application to the Authority to reconsider the decision to impose the financial penalty or the amount of the financial penalty so imposed in accordance with this section.

(3) Unless the Authority decides otherwise in any particular case, an application for reconsideration does not suspend the effect of the direction or decision to be reconsidered except in the case of an application for reconsideration under subsection (2).

(4) The application for reconsideration shall —

(a) subject to subsection (5), be submitted to the Authority within the prescribed period;

(b) be made in the form and manner required by the Authority; and

(c) set out the grounds on which the applicant is requesting the reconsideration.

(5) The Authority may, on written application by the organisation or an individual concerned, whether before, on or after the expiry of the prescribed period mentioned in subsection (4)(a), extend the time for the organisation or the individual to make the application for reconsideration if the Authority is satisfied that the extension should be granted by reason of exceptional circumstances in the particular case.

(6) If an application for reconsideration is made in accordance with this section, the Authority shall —

(a) reconsider the direction or decision;

(b) take any of the following actions as the Authority thinks fit —

(i) affirm, revoke or vary the direction or decision;

(ii) affirm or revoke, or vary the amount of, the financial penalty; and

(c) notify the applicant in writing of the result of the reconsideration.

(7) There is to be no application for reconsideration of a decision made under subsection (6)(b).

PART 10

APPEALS

Data Protection Appeal Panel and Data Protection Appeal Committee

41. (1) There is established a Data Protection Appeal Panel consisting of —

(a) a Chairman; and

(b) not more than thirty members,

appointed by the Minister on the basis of their ability and experience in industry, commerce or administration or their professional qualifications or their suitability otherwise for appointment.

(2) For the purpose of hearing any appeal under section 42, the Chairman of the Appeal Panel may nominate three or more members of the Appeal Panel, which may include the Chairman of the Appeal Panel, to constitute a Data Protection Appeal Committee.

(3) Schedule 6 has effect with respect to the Appeal Panel, Appeal Committee and their members and the proceedings.

Appeal from direction or decision of Authority

42. (1) An organisation or a person (including an individual who is a complainant) aggrieved by —

(a) any direction made by the Authority under section 34(2), 36(1) or (2) or 39(4);

(b) any direction or decision made by the Authority under section 35(2); or

(c) any decision made by the Authority under section 40(6)(b),

may, within the prescribed period, appeal to the Chairman of the Appeal Panel against that direction or decision.

(2) An organisation aggrieved by a financial penalty imposed by the Authority under section 37(1) on the organisation may, within the prescribed period, appeal to the Chairman of the Appeal Panel against the decision to impose the financial penalty or the amount of the financial penalty so imposed.

(3) Where an application for reconsideration has been made under section 40, every appeal in respect of the same direction or decision which is the subject of the application for reconsideration is deemed to be withdrawn.

(4) Unless the Appeal Committee decides otherwise in any particular case, the making of an appeal under this section does not suspend the effect of the direction or decision to which the appeal relates except in the case of an appeal under subsection (2).

(5) An Appeal Committee hearing an appeal may confirm, vary or set aside the direction or decision which is the subject of the appeal and, in particular, may –

(a) remit the matter to the Authority;

(b) impose or revoke, or vary the amount of, a financial penalty;

(c) give any direction, or take any other step, that the Authority could itself have given or taken; or

(d) make any other direction or decision that the Authority could itself have made.

(6) A direction or decision of an Appeal Committee on an appeal has the same effect, and may be enforced in the same manner, as a direction or decision of the Authority, except that there is to be no application for further reconsideration under section 40 and no further appeal under this section from the direction or decision of the Appeal Committee.

(7) If an Appeal Committee confirms the direction or decision which is the subject of the appeal, it may nevertheless set aside any finding of fact on which the direction or decision was based.

(8) The decision of an Appeal Committee is final.

PART 11

INVESTIGATION AND OFFENCES

Powers of investigation

43. (1) The Authority may, on complaint or of its own motion, conduct an investigation under this section to determine whether or not an organisation is complying with this Order, including a voluntary undertaking given under section 39.

(2) The Authority may suspend, discontinue or refuse to conduct an investigation under this section if it thinks fit, including but not limited to any of the following circumstances —

(a) the complainant has not complied with a direction under section 34(2);

(b) the parties involved in the matter have mutually agreed to settle the matter;

(c) any party involved in the matter has commenced legal proceedings against another party in respect of any contravention or alleged contravention of this Order by the other party;

(d) the Authority accepts a voluntary undertaking given by an organisation under section 39(1) in relation to the matter;

(e) the Authority is of the opinion that the matter may be more appropriately investigated by another regulatory authority and has referred the matter to that authority; or

(f) the Authority is of the opinion that —

(i) a complaint is frivolous or vexatious or is not made in good faith; or

(ii) any other circumstances warrant refusing to conduct, suspending or discontinuing the investigation.

(3) For the avoidance of doubt, notwithstanding subsection (2)(d), the Authority may conduct or resume an investigation under this section at any time if an organisation fails to comply with a voluntary undertaking given under section 39(1) in relation to any matter.

(4) An organisation shall retain records relating to an investigation under this section for one year after the conclusion of the investigation or any longer period specified in writing by the Authority.

Power to require documents or information

44. (1) For the purposes of an investigation under section 43, the Authority or any authorised officer may, by notice in writing to any organisation, require the organisation to produce to the Authority or the authorised officer a specified document or specified information, which the Authority or authorised officer considers relates to any matter relevant to such investigation.

(2) A notice under subsection (1) shall indicate the purpose for which the specified document or specified information is required by the Authority.

(3) The Authority may specify in the notice —

(a) the time and place at which any document is to be produced or any information is to be provided; and

(b) the manner and form in which it is to be produced or provided.

(4) The power under this section to require an organisation to produce a document includes the power —

(a) if the document is produced —

(i) to take copies of it or extracts from it; and

(ii) to require such organisation, or any person who is a present or past officer of the organisation, or is or was at any time employed by the organisation, to provide an explanation of the document; or

(b) if the document is not produced, to require such organisation or person to state, to the best of his knowledge and belief, where it is.

(5) In subsections (1) and (2), "specified" means —

(a) specified or described in the notice; or

(b) falling within a category which is specified or described in the notice.

Power to require provision of information etc.

45. (1) For the purposes of an investigation under section 43, the Authority or any authorised officer may do all or any of the following —

(a) require, by notice in writing, any person whom the Authority or authorised officer reasonably believes has any information, or any document in custody or control of the person, that is relevant to the investigation, to furnish that information or document, within the time and manner specified in the notice in writing;

(b) require, by notice in writing, any person within the limits of Brunei Darussalam, who appears to be acquainted with the facts or

circumstances of the matter, to attend before the Authority or authorised officer;

(c) examine orally any person who appears to be acquainted with the facts or circumstances of the matter.

(2) A person examined under subsection (1)(c) is bound to state truly the facts and circumstances with which the person is acquainted concerning the matter except that the person need not say anything that might expose the person to a criminal charge, penalty or forfeiture.

(3) A statement made by a person examined under subsection (1)(c) shall be —

(a) reduced to writing;

(b) read over to the person;

(c) if the person does not understand English, interpreted in a language that the person understands; and

(d) after correction (if necessary), signed by the person.

Power to enter premises without warrant

46. (1) In connection with an investigation under section 43, an authorised officer, and such other persons as the authorised officer may require to assist him, may enter any premises.

(2) No authorised officer or person assisting the authorised officer shall enter any premises in exercise of the powers under this section unless the authorised officer has given the occupier of the premises a notice in writing which —

(a) gives at least 2 working days' notice of the intended entry; and

(b) indicates the subject matter and purpose of the investigation.

(3) Subsection (2) does not apply if the authorised officer has reasonable grounds for suspecting that the premises are, or have been, occupied by an organisation which is being investigated in relation to a contravention of this Order and if the authorised officer has taken all such steps as are reasonably practicable to give notice in writing under that subsection but has not been able to do so.

(4) Where subsection (3) applies, the power of entry conferred by subsection (1) shall be exercised on production of —

(a) evidence of the authorised officer's appointment; and

(b) a document containing the information referred to in subsection (2)(b).

(5) An authorised officer or a person assisting the authorised officer entering any premises under this section may —

(a) take with him such equipment as appears to him to be necessary;

(b) require any person on the premises —

(i) to produce any document which he considers relates to any matter relevant to the investigation; and

(ii) if the document is produced, to provide an explanation of it;

(c) require any person to state, to the best of the person's knowledge and belief, where any such document is to be found;

(d) take copies of, or extracts from, any document which is produced;

(e) require any information which is stored in any electronic form and is accessible from the premises and which he considers relates to any matter relevant to the investigation, to be produced in a form —

(i) in which it can be taken away; and

(ii) in which it is visible and legible; and

(f) take any step which appears to be necessary for the purpose of preserving or preventing interference with any document which he considers relates to any matter relevant to the investigation.

Power to enter premises under warrant

47. (1) The Authority or any authorised officer may apply to a court for a warrant and the court may issue such a warrant if it is satisfied that —

(a) there are reasonable grounds for suspecting that there are, on any premises, documents —

(i) the production of which has been required under section 44, 45 or 46; and

(ii) which have not been produced as required;

(b) there are reasonable grounds for suspecting that —

(i) there are, on any premises, documents which the Authority or the authorised officer has power under section 44 to require to be produced; and

(ii) if the documents were required to be produced, they would not be produced but would be concealed, removed, tampered with or destroyed; or

(c) an authorised officer or a person assisting the authorised officer has attempted to enter the premises in the exercise of his powers under section 46 but has been unable to do so and that there are reasonable grounds for suspecting that there are, on the premises, documents the production of which could have been required under that section.

(2) A warrant under this section shall authorise a named officer, and such other persons as the authorised officer may require to assist him, to do all or any of the following —

(a) to enter the premises specified in the warrant, using such force as is reasonably necessary for the purpose;

(b) to search any person on those premises if there are reasonable grounds for believing that the person has in his possession any document, equipment or article which has a bearing on the investigation;

(c) to search the premises and take copies of, or extracts from, any document appearing to be of a kind in respect of which the application under subsection (1) was granted (the relevant kind);

(d) to take possession of any document appearing to be of the relevant kind if —

(i) such action appears to be necessary for preserving the document or preventing interference with it; or

(ii) it is not reasonably practicable to take copies of the document on the premises;

(e) to take any other step which appears to be necessary for the purpose mentioned in paragraph (d)(i);

(f) to require any person to provide an explanation of any document appearing to be of the relevant kind or to state, to the best of his knowledge and belief, where it may be found;

(g) to require any information which is stored in any electronic form and is accessible from the premises and which he considers relates to any matter relevant to the investigation, to be produced in a form —

(i) in which it can be taken away; or

(ii) in which it is visible and legible; and

(h) to remove from those premises for examination any equipment or article which relates to any matter relevant to the investigation.

(3) If, in the case of a warrant under subsection (1)(b), the court is satisfied that it is reasonable to suspect that there are also on the premises other documents relating to the investigation concerned, the warrant shall also authorise the actions mentioned in subsection (2) to be taken in relation to any such document.

(4) Where possession of any document is taken under subsection (2)(d) or (3), the named officer may, at the request of the person from whom possession of the document was taken, provide such person with a copy of the document.

(5) A named officer may allow any equipment or article which has a bearing on an investigation and which may be removed from any premises for examination under subsection (2)(h) to be retained on those premises subject to such conditions as the named officer may require.

(6) A warrant issued under this section shall —

(a) indicate the subject matter and purpose of the investigation; and

(b) continue in force until the end of the period of one month beginning from the day on which it is issued.

(7) The powers conferred by this section shall not be exercised except on production of a warrant issued under this section.

(8) Any person entering any premises by virtue of a warrant under this section may take with him such equipment as appears to him to be necessary.

(9) If there is no one at the premises when the named officer proposes to execute such a warrant, he shall, before executing it —

(a) take such steps as are reasonable in all the circumstances to inform the occupier of the intended entry; and

(b) if the occupier is informed, afford him or his legal or other representative a reasonable opportunity to be present when the warrant is executed.

(10) If the named officer is unable to inform the occupier of the intended entry, he shall, when executing the warrant, leave a copy of the warrant in a prominent place on the premises.

(11) On leaving any premises which he has entered by virtue of a warrant under this section, the named officer shall, if the premises are unoccupied or the occupier is temporarily absent, leave them as effectively secured as he found them.

(12) Any document of which possession is taken under subsection (2)(d) or (3) may be retained for a period of not more than 3 months.

(13) In this section —

“named officer” means an authorised officer named in the warrant;

“occupier”, in relation to any premises, means a person whom the authorised officer reasonably believes is the occupier of those premises.

Offences and penalties

48. (1) Any person who —

(a) makes a request under section 18(1) to obtain access to personal data about another individual; or

(b) makes a request under section 19(1) to change personal data about another individual,

without the authority of the individual, is guilty of an offence and liable on conviction to a fine not exceeding \$5,000, imprisonment for a term not exceeding 12 months or both.

(2) An organisation or person who —

(a) with an intent to evade a request under section 18 or 19, disposes of, alters, falsifies, conceals or destroys, or directs another person to dispose of, alter, falsify, conceal or destroy, a record containing —

(i) personal data; or

(ii) information about the collection, use or disclosure of personal data;

(b) obstructs or hinders the Authority or an authorised officer in the performance of any function or duty, or the exercise of any power, under this Order;

(c) without reasonable excuse, neglects or refuses to provide any information or produce any document which the organisation or person is required by or under this Order to provide or produce to the Authority or an authorised officer;

(d) neglects or refuses to attend before the Authority or an authorised officer as required by or under this Order; or

(e) makes a statement, or furnishes any information or document, to the Authority or an authorised officer under this Order, which the organisation or person knows, or ought reasonably to know, to be false or misleading in any material particular,

is guilty of an offence and liable on conviction —

(i) in the case of an individual, to a fine not exceeding \$10,000, imprisonment for a term not exceeding 12 months or both; and

(ii) in any other case, to a fine not exceeding \$100,000.

General penalty

49. Any person who contravenes or fails to comply with any provision of this Order for which no penalty is expressly provided is guilty of an offence and liable on conviction to a fine not exceeding \$10,000, imprisonment for a term not exceeding 3 years or both and, in the case of a continuing offence, to a further fine not exceeding \$1,000 for every day or part thereof during which the offence continues after conviction.

Offences by body corporate etc.

50. (1) Where an offence under this Order committed by a body corporate is proved —

(a) to have been committed with the consent or connivance of an officer; or

(b) to be attributable to any neglect on his part,

the officer as well as the body corporate is guilty of that offence and liable to be proceeded against and punished accordingly.

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

(3) Where an offence under this Order committed by a partnership is proved —

(a) to have been committed with the consent or connivance of a partner; or

(b) to be attributable to any neglect on his part,

the partner as well as the partnership is guilty of that offence and liable to be proceeded against and punished accordingly.

(4) Where an offence under this Order committed by a limited liability partnership is proved —

(a) to have been committed with the consent or connivance of a partner or manager of the limited liability partnership; or

(b) to be attributable to any neglect on their part,

the partner or manager, as well as the partnership is guilty of that offence and liable to be proceeded against and punished accordingly.

(5) Where an offence under this Order committed by an unincorporated association (other than a partnership) is proved —

(a) to have been committed with the consent or connivance of; or

(b) to be attributable to any neglect on the part of,

an officer of the unincorporated association or a member of its governing body, the officer or member, as well as the unincorporated association is guilty of that offence and liable to be proceeded against and punished accordingly.

(6) A person mentioned in subsections (1), (2), (3), (4) and (5) may rely on a defence that would be available to the body corporate, partnership, limited liability partnership or unincorporated association if it were charged with the offence with which the person is charged and, in doing so, the person bears the same burden of proof that the body corporate, partnership, limited liability partnership or unincorporated association would bear.

(7) In this section, unless the context otherwise requires —

"officer" —

(a) in relation to a body corporate, means a director, member of the committee of management, chief executive, manager, secretary or other similar officer of the body corporate, any person who holds a controlling interest in that body, and includes a person purporting to act in any such capacity; or

(b) in relation to an unincorporated association (other than a partnership), means the president, the secretary or a member of the committee of the unincorporated association or a person holding a position analogous to that of president, secretary or member of a committee, and includes a person purporting to act in any such capacity;

"partner", in relation to a partnership, includes a person purporting to act as a partner.

Liability of employers for acts of employees

51. (1) Any act done or conduct engaged in by a person in the course of his employment (referred to in this section as the employee) is treated for the purposes of this Order as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.

(2) In any proceedings for an offence under this Order brought against any person in respect of an act or conduct alleged to have been done or engaged in by an employee of that person, it is a defence for that person to prove that he took such steps as were practicable to prevent the employee from doing the act or

engaging in the conduct, or from doing or engaging in, in the course of his employment, acts or conduct, of that description.

Composition of offences

52. (1) The Authority or any person authorised in writing in that behalf by the Authority may compound any offence against this Order which is prescribed as a compoundable offence by collecting from the person reasonably suspected of having committed the offence a sum not exceeding —

(a) one half of the amount of the maximum fine prescribed for the offence; or

(b) \$5,000,

whichever is the lower.

(2) On payment of the sum of money, no further proceedings shall be taken against the person in respect of the offence.

(3) All sums collected under this section shall be paid to the Authority.

PART 12

GENERAL

Conduct of proceedings

53. Notwithstanding the provisions of any written law —

(a) in any civil proceedings by or against the Authority; or

(b) in any other civil proceedings in which the Authority is required or permitted by the court to be represented, or to be heard, or is otherwise entitled to be represented or to be heard,

any person authorised or appointed by the Authority for that purpose may —

(i) appear in any civil proceedings involving the performance of any function or duty, or the exercise of any power, of the Authority under any written law; and

(ii) make all applications and do all acts in respect of the civil proceedings on behalf of the Authority or an authorised officer.

Cooperation agreements

54. (1) For the purposes of section 60, a cooperation agreement is an agreement for the purposes of —

(a) facilitating cooperation between the Authority and another regulatory authority in the performance of their respective functions in so far as those functions relate to data protection; and

(b) avoiding duplication of activities by the Authority and another regulatory authority, being activities involving the enforcement of data protection laws.

(2) A cooperation agreement may include provisions —

(a) to enable the Authority and the other regulatory authority to furnish to each other information in their respective possession if the information is required by the other for the purpose of performance by it of any of its functions;

(b) to provide such other assistance to each other as will facilitate the performance by the other of any of its functions; and

(c) to enable the Authority and the other regulatory authority to forbear to perform any of their respective functions in relation to a matter in circumstances where it is satisfied that the other is performing functions in relation to that matter.

(3) The Authority shall not furnish any information to a foreign data protection body pursuant to a cooperation agreement unless it requires of, and obtains from, that body an undertaking in writing by it that it will comply with terms specified in that requirement, including terms that correspond to the provisions of any written law concerning the disclosure of that information by the Authority.

(4) The Authority may give an undertaking to a foreign data protection body that it will comply with terms specified in a requirement made of the Authority by the foreign data protection body to give such an undertaking where —

(a) those terms correspond to the provisions of any written law in force in the country or territory in which the foreign data protection body is established, being provisions which concern the disclosure by the foreign data protection body of the information referred to in paragraph (b); and

(b) compliance with the requirement is a condition imposed by the foreign data protection body for furnishing information in its possession to the Authority pursuant to a cooperation agreement.

(5) In this section —

“foreign data protection body” means a body in whom there are vested functions under the law of another country or territory with respect to the enforcement or the administration of provisions of law of that country or territory concerning data protection;

“regulatory authority” includes the Authority and any foreign data protection body.

Advisory guidelines

55. (1) The Authority may issue written advisory guidelines and other guidance documents as it may consider desirable in respect of any particular provision of this Order.

(2) Any guidelines issued under this section may be varied, amended or revoked by the Authority.

(3) The Authority shall publish the guidelines in any way the Authority thinks fit, but failure to comply with this subsection in respect of any guideline does not invalidate the guidelines.

Certificate as to national interest

56. For the purposes of this Order, if any doubt arises as to whether anything is necessary for the purpose of, or could be contrary to, the national interest, a certificate signed by the Minister responsible for that matter is conclusive evidence of the matters stated therein.

Evidence in proceedings

57. (1) The Authority, the Appeal Panel, an Appeal Committee, their members and anyone acting for or under the direction of the Authority shall not give or be compelled to give evidence in a court or in any other proceedings in respect of any information obtained in performing their duties or exercising their powers or functions under this Order, except —

(a) in a prosecution for perjury or for the furnishing of false information; or

(b) in a prosecution for an offence under this Order.

(2) Subsection (1) applies also in respect of evidence of the existence of proceedings conducted before the Authority.

Enforcement of directions or decisions in High Court

58. (1) Subject to subsection (3), where —

(a) a direction has been made by the Authority under section 36(1); or

(b) a decision to impose the financial penalty has been made by the Authority under section 37(1),

and the organisation against whom it is made fails to comply therewith, the Authority may send a certified copy thereof to the High Court.

(2) The High Court shall cause the certified copy to be recorded and thereon the direction or decision shall for all purposes be enforceable as a judgment of a High Court.

(3) For the purposes of this section, if the organisation —

(a) makes an application for reconsideration to the Authority in accordance with section 40; or

(b) appeals to the Chairman of the Appeal Panel under section 42,

the Authority may send a certified copy of the direction or decision until after the result of the reconsideration or determination of the appeal, as the case may be.

Right of private action

59. (1) A person who suffers loss or damage directly as a result of a contravention by an organisation of any provision of Part 4, 5, 6 or 7 has a right of action for relief in civil proceedings in a court.

(2) If the Authority has made a decision under this Order in respect of a contravention specified in subsection (1), an action accruing under subsection (1) may not be brought in respect of that contravention until after the decision has become final as a result of there being no further right of appeal.

(3) The court may grant to the plaintiff in an action under subsection (1) all or any of the following —

(a) relief by way of injunction or declaration;

(b) damages;

(c) any other relief as the court thinks fit.

Preservation of secrecy

60. (1) Subject to subsection (5), every specified person shall preserve, and aid in the preservation of, secrecy with regard to —

(a) any personal data an organisation would be required or authorised to refuse to disclose if it were contained in personal data requested under section 18;

(b) whether information exists, if an organisation in refusing to provide access under section 18 does not indicate whether the information exists;

(c) all matters that have been identified as confidential under subsection (3); and

(d) all matters relating to the identity of persons furnishing information to the Authority,

that may come to his knowledge in the performance of his functions and discharge of his duties under this Order and shall not communicate any such matter to any person, except in so far as such communication —

(i) is necessary for the performance of any such function or discharge of any such duty; or

(ii) is lawfully required by any court, or lawfully required or permitted under this Order, or any other written law.

(2) Any person who fails to comply with subsection (1) is guilty of an offence.

(3) Any person, when furnishing any information to the Authority, may identify information that he claims to be confidential information.

(4) Every claim made under subsection (3) shall be supported by a written statement giving reasons why the information is confidential.

(5) Notwithstanding subsection (1), the Authority may disclose, or authorise any specified person to disclose, any information relating to any matter referred to in subsection (1) in any of the following circumstances —

(a) where the consent of the person to whom the information relates has been obtained;

(b) if the Authority considers there is evidence of an offence, disclose information relating to the commission of an offence to the Public Prosecutor, any police officer and other law enforcement authorities;

(c) to give effect to any provision of this Order;

(d) for the purposes of a prosecution, an application or an appeal referred to in section 57(1)(a) or (b);

(e) to comply with any provision of a cooperation agreement entered into under section 54, where the conditions specified in subsection (6) are satisfied; or

(f) to a public body in any circumstances as the Authority may determine.

(6) The conditions referred to in subsection (5)(e) are —

(a) that the information or documents requested by the foreign country are in the possession of the Authority;

(b) that unless the Government otherwise allows, the foreign country undertakes to keep the information given confidential at all times; and

(c) that the disclosure of the information is not likely to be contrary to the public interest.

(7) In this section —

“specified person” means a person who is or has been —

(a) a member or an officer of a relevant body;

(b) a person authorised or appointed by a relevant body to perform the relevant body's functions or duties, or exercise the relevant body's powers, under this Order or any other written law;

(c) a member of a committee of a relevant body or any person authorised, appointed or employed to assist the relevant body; or

(d) an authorised officer or a person authorised, appointed or employed to assist an authorised officer;

"relevant body" means the Authority, the Appeal Panel or an Appeal Committee.

Protection from personal liability

61. No liability shall lie personally against the Authority, the Appeal Panel, an Appeal Committee and their members or any other persons acting under the direction of the Authority, the Appeal Panel or an Appeal Committee for anything done or intended to be done in good faith and with reasonable care in the execution or purported execution of this Order.

Public servants

62. All members of the advisory committee, Appeal Panel and Appeal Committee are deemed to be public servants for the purposes of the Penal Code (Chapter 22).

Exemption

63. The Authority may, with the approval of the Minister, by order published in the *Gazette*, exempt any individual or organisation or any class of individuals or organisations from all or any of the provisions of this Order, subject to such conditions or restrictions as the Minister may impose.

Amendment of Schedules

64. The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, by order published in the *Gazette*, amend the Schedules.

Regulations

65. (1) The Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, make such regulations as he considers necessary or expedient for giving effect to or carrying out the provisions of this Order, including the prescription of fees and other things required to be or which may be prescribed under this Order, and for the due administration thereof.

(2) Without prejudice to the generality of subsection (1), the Minister may, with the consent of His Majesty the Sultan and Yang Di-Pertuan, make regulations for or with respect to all or any of the following matters —

(a) the form, manner and procedures, relating to the making and responding to requests under section 18 or 19, including the content of responses to such requests, the period for such responses, the circumstances in which an organisation may refuse to provide a response

or refuse to confirm or deny the existence of any matter and the fees that an organisation may charge in respect of such requests;

(b) the assessment and notification of notifiable data breaches, including —

- (i) the steps and measures that an organisation shall take in relation to the investigation and assessment of data breaches; and
- (ii) the form and manner in which the Authority and affected individuals shall be notified of notifiable data breaches;

(c) the classes of persons who may act under this Order for minors, deceased persons or any other individuals who lack capacity to act under this Order and regulating the manner in which, and the extent to which, any rights or powers of individuals under this Order may be exercised on their behalf;

(d) the form, manner and procedures relating to applications and complaints under this Order;

(e) to provide for matters relating to the operation by an operator of a dispute resolution scheme, including —

- (i) the standards or requirements of the services provided under the dispute resolution scheme;
- (ii) the fees that the operator may charge for the services provided under the dispute resolution scheme;
- (iii) the records that the operator shall keep, and the period of retention of those records;
- (iv) the reports that the operator shall submit to the Authority, and the manner and time for those submissions; and
- (v) generally to give effect to or for carrying out the purposes of section 34;

(f) the conduct of reviews by the Authority under section 35;

(g) the form, manner and procedures for applications for reconsideration by the Authority under section 40;

(h) the form, manner and procedures for appeals to an Appeal Committee, including the fees to be paid in respect of such appeals;

(i) the award of costs of or incidental to any proceedings before the Authority or Appeal Committee, and the award of expenses, including any allowance payable to persons in connection with their attendance before the Authority or Appeal Committee;

(j) the fees to be paid in respect of applications, and services provided by or on behalf of the Authority, under this Order.

SCHEDULE 1
(section 14(1) and Schedule 3)

**COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA
WITHOUT CONSENT**

PART 1

VITAL INTERESTS OF INDIVIDUALS

1. (1) Subject to sub-paragraph (2), the collection, use or disclosure of personal data about an individual is necessary for any purpose which is clearly in the interests of the individual, if —

(a) consent for the collection, use or disclosure cannot be obtained in a timely way; or

(b) the individual would not reasonably be expected to withhold consent.

(2) Where the organisation collects, uses or discloses personal data about the individual under sub-paragraph (1), the organisation shall, as soon as is practicable, notify the individual of the collection, use or disclosure and the purpose for the collection, use or disclosure.

2. The collection, use or disclosure of personal data about an individual is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual.

3. The collection, use or disclosure of personal data about an individual where —

(a) consent for the collection, use or disclosure of personal data about an individual cannot be obtained in a timely way; and

(b) there are reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected.

4. The collection, use or disclosure of personal data is for the purpose of contacting the next of kin or a friend of any injured, ill or deceased individual.

PART 2

MATTERS AFFECTING PUBLIC

1. The collection, use or disclosure of personal data about an individual that is publicly available.
2. The collection, use or disclosure of personal data about an individual is in the national interest.
3. The collection, use or disclosure of personal data about an individual is solely for artistic or literary purposes.
4. The collection, use or disclosure of personal data about an individual is solely for archival or historical purposes if a reasonable person would not consider the personal data to be too sensitive to the individual to be collected, used or disclosed at the proposed time.
5. The personal data about an individual is collected, used or disclosed by a news organisation solely for its news activity.
6. In this Part —

"broadcasting service" has the same meaning assigned to it under section 2 of the Broadcasting Act (Chapter 180);

"news activity" means —

(a) the gathering of news, or the preparation or compilation of articles or programmes of or concerning news, observations on news, or current affairs, for the purposes of dissemination to the public or any section of the public; or

(b) the dissemination, to the public or any section of the public, of any article or programme of or concerning —

(i) news;

(ii) observations on news; or

(iii) current affairs;

"news organisation" means —

(a) any organisation —

(i) the business of which consists, in whole or in part, of news activity carried out in relation to a relevant broadcasting service, a newswire service or the publication of a newspaper; and

(ii) which publishes a newspaper in Brunei Darussalam within the meaning of the Newspapers Act (Chapter 105); or

(b) any organisation which provides a broadcasting service in or from Brunei Darussalam and holds a broadcasting licence granted under the Broadcasting Act (Chapter 180);

"newspaper" has the same meaning assigned to it under section 2 of the Newspapers Act (Chapter 105);

"relevant broadcasting service" means any of the following licensable broadcasting services having the same meaning assigned to it in the Broadcasting Act (Chapter 180) —

(a) free-to-air nationwide television services;

(b) free-to-air localised television services;

(c) free-to-air international television services;

(d) subscription nationwide television services;

(e) subscription localised television services;

(f) subscription international television services;

(g) special interest television services;

(h) free-to-air nationwide radio services;

(i) free-to-air localised radio services;

(j) free-to-air international radio services;

(k) subscription nationwide radio services;

- (l)* subscription localised radio services;
- (m)* subscription international radio services;
- (n)* special interest radio services.

PART 3

LEGITIMATE INTERESTS

1. (1) Subject to sub-paragraphs (2), (3) and (4) —

(a) the collection, use or disclosure of personal data about an individual is in the legitimate interests of the organisation or another person; and

(b) the legitimate interests of the organisation or other person outweigh any adverse effect on the individual.

- (2) For the purposes of sub-paragraph (1), the organisation shall —

(a) conduct an assessment, before collecting, using or disclosing the personal data to determine whether sub-paragraph (1) is satisfied; and

(b) provide the individual with reasonable access to information about the organisation's collection, use or disclosure of personal data in accordance with sub-paragraph (1).

- (3) The organisation shall, in respect of the assessment mentioned in sub-paragraph (2)*(a)* —

(a) identify any adverse effect that the proposed collection, use or disclosure of personal data about an individual is likely to have on the individual;

(b) identify and implement reasonable measures —

- (i)* to eliminate the adverse effect;
- (ii)* to reduce the likelihood that the adverse effect will occur; or
- (iii)* to mitigate the adverse effect; and

(c) comply with any other prescribed requirements.

(4) Sub-paragraph (1) does not apply to the collection, use or disclosure of personal data about an individual for the purpose of sending to that individual or any other individual a direct marketing message.

2. The collection, use or disclosure of personal data about an individual is necessary for evaluative purposes.

3. The collection, use or disclosure of personal data about an individual is necessary for any investigation or proceedings.

4. The collection, use or disclosure of personal data about an individual is necessary for the organisation —

(a) to recover a debt owed by the individual to the organisation; or

(b) to pay to the individual a debt owed by the organisation.

5. The collection, use or disclosure of personal data about an individual is necessary for the provision of legal services by the organisation to another person, or for the organisation to obtain legal services.

6. (1) Subject to sub-paragraph (2), the collection, use or disclosure of personal data about an individual —

(a) is for the purpose of the preparation by a credit bureau of a credit report; or

(b) relates to a credit report provided by a credit bureau to a member of the credit bureau in relation to a transaction between the member and the individual.

(2) Sub-paragraph (1) does not apply to a credit bureau that, being required to obtain a licence under any other written law, does not hold such a licence.

7. The collection, use or disclosure of personal data about an individual is to —

(a) confer an interest or a benefit on the individual under a private trust or benefit plan; and

(b) administer that trust or benefit plan, at the request of the settlor or the person establishing the benefit plan.

8. The personal data about an individual —

(a) is provided to the organisation by another individual, or by an organisation to which the personal data had been provided by another individual, to enable the organisation to provide a service for the personal or domestic purposes of that other individual; and

(b) is collected, used or disclosed by the organisation solely for the purpose in sub-subparagraph *(a)*.

9. The personal data about an individual —

(a) is included in a document produced in the course, and for the purposes, of the individual's employment, business or profession; and

(b) is collected, used or disclosed for purposes consistent with the purpose for which the document was produced.

10. The personal data about an individual is collected, used or disclosed by the organisation, and the collection, use or disclosure of the personal data is reasonable for the purpose of or in relation to the organisation —

(a) entering into an employment relationship with the individual or appointing the individual to any office; or

(b) managing or terminating the employment relationship with or appointment of the individual.

11. In this Part, "benefit plan" means an insurance policy, a pension plan, an annuity, a provident fund plan or other similar plan.

PART 4

BUSINESS ASSET TRANSACTIONS

1. (1) Subject to the conditions in sub-paragraphs (2), (3), (4) and (5), where an organisation (*X*) is a party or a prospective party to a business asset transaction with another organisation (*Y*), personal data about an applicable individual of *Y* —

(a) is collected from *Y* by *X* for the purpose of the business asset transaction;

(b) is used or disclosed by *X* in relation to the business asset transaction; or

(c) is disclosed by *Y* to *X* for the purposes of the business asset transaction.

(2) Where the business asset transaction concerns any part of *Y* or *Y*'s business assets, the personal data mentioned in sub-paragraph (1) shall relate directly to *Y* or *Y*'s business assets.

(3) If *X* is a prospective party to the business asset transaction, the following conditions apply –

(a) *X* may collect, and *Y* may disclose, only personal data that is necessary for *X* to determine whether to proceed with the business asset transaction; and

(b) *X* and *Y* shall have entered into an agreement that requires *X* to use or disclose the personal data solely for purposes related to the business asset transaction.

(4) If *X* enters into the business asset transaction, the following conditions apply –

(a) *X* may use or disclose the personal data *X* collected from *Y* only for the same purposes for which *Y* would have been permitted to use or disclose the personal data;

(b) if any personal data *X* collects from *Y* does not relate directly to the part of *Y* or *Y*'s business assets with which the business asset transaction entered into is concerned, *X* shall destroy, or return to *Y*, that personal data;

(c) *X* or *Y* shall notify the applicable individuals of *Y* whose personal data is disclosed that –

(i) the business asset transaction has taken place; and

(ii) the personal data about them has been disclosed to *X*.

(5) If the business asset transaction does not proceed or is not completed, *X* shall destroy, or return to *Y*, all personal data collected.

2. (1) Subject to the conditions in sub-paragraphs (2), (3) and (4), where an organisation (*X*) is a party or a prospective party to a business asset transaction with another organisation (*Y*) in respect of *Y*'s interest in a third organisation (*Z*) (referred to in this paragraph as the relevant transaction), personal data about an applicable individual of *Z* –

(a) is collected from *Y* by *X* for the purposes of the business asset transaction;

(b) is used or disclosed by *X* in relation to the business asset transaction; or

(c) is disclosed by *Y* to *X* for the purposes of the business transaction.

(2) If *X* is a prospective party to the relevant transaction, the following conditions apply —

(a) where *X* collects the personal data mentioned in sub-paragraph (1) from *Y* or *Z* —

- (i) *X* may collect, and *Y* or *Z* may disclose, only personal data that is necessary for *X* to determine whether to proceed with the relevant transaction; and
- (ii) *X* and *Y* or *Z* shall have entered into an agreement that requires *X* to use or disclose the personal data solely for purposes related to the relevant transaction;

(b) where *Y* collects the personal data mentioned in sub-paragraph (1) from *Z* —

- (i) *Y* may collect, and *Z* may disclose, only personal data that is necessary for *X* or *Y* to determine whether to proceed with the relevant transaction; and
- (ii) *Y* and *Z* should have entered into an agreement that requires *Y* to use or disclose the personal data solely for purposes related to the relevant transaction.

(3) If *X* enters into the relevant transaction, the following conditions apply —

(a) *X* may use or disclose the personal data collected from *Y* or *Z* only for the same purposes for which *Y* or *Z* would have been permitted to use or disclose the personal data;

(b) *Y* may use or disclose the personal data collected from *Z* only for the same purposes for which *Z* would have been permitted to use or disclose the personal data;

(c) X, Y or Z shall notify the applicable individuals of Z whose personal data is disclosed that —

(i) the relevant transaction has taken place; and

(ii) the personal data about them has been disclosed to X.

(4) If the relevant transaction does not proceed or is not completed —

(a) X shall destroy, or return to Y or Z, all personal data collected; and

(b) Y shall destroy, or return to Z, all personal data collected.

3. In this Part —

"applicable individual", in relation to an organisation, includes a contractor, a customer, a director, an employee, an officer or a shareholder of the organisation;

"business asset transaction" —

(a) means the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of —

(i) an organisation or a portion of an organisation;

(ii) an interest in an organisation; or

(iii) any of the business or assets of an organisation, other than any personal data to be disclosed under paragraph 1(1) or 2(1); and

(b) includes —

(i) the amalgamation of a corporation with one or more related corporations; and

(ii) the transfer or disposal of any of the business or assets of a corporation to a related corporation;

"interest" means —

(a) in relation to a corporation, a share in that corporation;

(b) in relation to an entity other than a corporation, any right or interest (whether legal or equitable) in that entity, by whatever name called;

(c) in relation to a trust business, a unit in that trust business; and

(d) in relation to a trust other than a trust business, any right or interest (whether legal or equitable) in that trust, by whatever name called.

PART 5

BUSINESS IMPROVEMENT PURPOSES

1. (1) Subject to the conditions in sub-paragraphs (3), (4) and (5), personal data about an individual (*P*) —

(a) is collected by an organisation (*X*) that is a corporation from a related corporation (*Y*) for a purpose specified in sub-paragraph (2) (referred to in this paragraph as the relevant purpose);

(b) is used by *X* for a relevant purpose; or

(c) is disclosed by *Y* to *X* for a relevant purpose.

(2) The relevant purposes mentioned in sub-paragraph (1) are the following —

(a) improving or enhancing any goods or services provided, or developing new goods or services to be provided, by *X* or *Y*;

(b) improving or enhancing the methods or processes, or developing new methods or processes, for the operations of *X* or *Y*;

(c) learning about and understanding the behaviour and preferences of *P* or another individual in relation to the goods or services provided by *X* or *Y*;

(d) identifying any goods or services provided by *X* or *Y* that may be suitable for *P* or another individual, or personalising or customising any such goods or services for *P* or another individual.

(3) Sub-paragraph (1)*(a)* and *(c)* applies only if —

(a) the relevant purpose for which *X* collects, or *Y* discloses, personal data about *P* cannot reasonably be achieved without the collection, use or disclosure of the personal data in an individually identifiable form;

(b) a reasonable person would consider the collection or disclosure of personal data about *P* for the relevant purpose to be appropriate in the circumstances; and

(c) *X* and *Y* are bound by any contract or other agreement or binding corporate rules requiring the recipient of personal data about *P* to implement and maintain appropriate safeguards for the personal data.

(4) Sub-paragraph (1)*(b)* applies only if —

(a) the relevant purpose for which *X* uses personal data about *P* cannot reasonably be achieved without the use of the personal data in an individually identifiable form; and

(b) a reasonable person would consider the use of personal data about *P* for the relevant purpose to be appropriate in the circumstances.

(5) Where *X* collects from *Y*, and *Y* discloses to *X*, personal data about *P* for a purpose mentioned in sub-paragraph (2)*(c)* or *(d)*, *P* shall be, at the time of the collection or disclosure —

(a) an existing customer of *Y*; and

(b) an existing customer or a prospective customer of *X*.

(6) For the avoidance of doubt, sub-paragraph (1) does not apply to the collection, use or disclosure of personal data about *P* for the purpose of sending to *P* or another individual a direct marketing message.

2. In this Part —

"existing customer", in relation to a corporation, means an individual who purchases, hires or uses, or has purchased, hired or used, any goods or services provided by the corporation;

"prospective customer of *X*" means an individual who, at the time mentioned in paragraph 1(5) –

(a) has informed *X* of the individual's interest in purchasing, hiring or using any goods or services provided by *X*; or

(b) is conducting negotiations with *X* that lead or may lead to an agreement between the individual and *X* for the purchase, hire or use of any goods or services provided by *X*.

SCHEDULE 2
(sections 2(1) and 14(1))

**ADDITIONAL BASES FOR COLLECTION, USE AND DISCLOSURE OF
PERSONAL DATA WITHOUT CONSENT**

PART 1

COLLECTION OF PERSONAL DATA

The collection of personal data about an individual, if —

- (a)* the personal data was disclosed by a public agency; and
- (b)* the collection of the personal data by the organisation is consistent with the purpose of the disclosure by the public agency.

PART 2

USE OF PERSONAL DATA

Division 1

Public interest

1. The use of personal data about an individual, if —

- (a)* the personal data was disclosed by a public agency; and
- (b)* the use of the personal data by the organisation is consistent with the purpose of the disclosure by the public agency.

Division 2

Business improvement purposes

2. (1) Subject to the conditions in sub-paragraph (2), personal data about an individual (*P*) is used by the organisation for any of the following purposes —

- (a)* improving or enhancing any goods or services provided, or developing new goods or services to be provided, by the organisation;

(b) improving or enhancing the methods or processes, or developing new methods or processes, for the operations of the organisation;

(c) learning about and understanding the behaviour and preferences of *P* or any other individual in relation to the goods or services provided by the organisation;

(d) identifying any goods or services provided by the organisation that may be suitable for *P* or another individual, or personalising or customising any such goods or services for *P* or another individual.

(2) Sub-paragraph (1) applies only if —

(a) the purpose for which the organisation uses personal data about *P* cannot reasonably be achieved without the use of the personal data in an individually identifiable form; and

(b) a reasonable person would consider the use of personal data about *P* for that purpose to be appropriate in the circumstances.

(3) For the avoidance of doubt, sub-paragraph (1) does not apply to the use of personal data about *P* for the purpose of sending to *P* or another individual a direct marketing message.

(4) In this paragraph, "organisation" does not include a corporation within the meaning given by section 2(1) of the Companies Act (Chapter 39).

Division 3

Research

3. The use of personal data about an individual for a research purpose including historical or statistical research, if —

(a) the research purpose cannot reasonably be accomplished unless the personal data is used in an individually identifiable form;

(b) there is a clear public benefit to using the personal data for the research purpose;

(c) the results of the research will not be used to make any decision that affects the individual; and

(d) in the event that the results of the research are published, the organisation publishes the results in a form that does not identify any individual.

PART 3

DISCLOSURE OF PERSONAL DATA WITHOUT CONSENT

Division 1

Public interest

1. The disclosure of personal data about an individual to a public agency where the disclosure is necessary in the public interest.
2. The disclosure of personal data about an individual who is a current or former student of an educational institution to a public agency for the purposes of policy formulation or review.
3. The disclosure of personal data about an individual who is a current or former patient of any prescribed healthcare body to a public agency for the purposes of policy formulation or review.
4. The disclosure of personal data about any individual to any officer of a prescribed law enforcement agency, on production of written authorisation signed by the head or director of that prescribed law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

Division 2

Research

5. The disclosure of personal data about an individual for a research purpose including historical or statistical research, if —
 - (a) the research purpose cannot reasonably be accomplished unless the personal data is disclosed in an individually identifiable form;
 - (b) it is impracticable for the organisation to seek the consent of the individual for the disclosure;
 - (c) there is a clear public benefit to disclosing the personal data for the research purpose;

(d) the results of the research will not be used to make any decision that affects the individual; and

(e) in the event that the results of the research are published, the organisation shall publish the results in a form that does not identify any individual.

SCHEDULE 3

(section 18(2))

EXCEPTIONS FROM ACCESS REQUIREMENT

1. An organisation is not required to provide information under section 18(1) in respect of –

(a) opinion data kept solely for an evaluative purpose;

(b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

(c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

(d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

(e) a document related to a prosecution if all proceedings related to the prosecution have not been completed;

(f) personal data which is subject to legal privilege;

(g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;

(h) personal data collected, used or disclosed without consent, under paragraph 3 of Part 3 of Schedule 1, for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed;

(i) the personal data was collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration for which he was appointed to act –

(i) by agreement between the parties to the mediation or arbitration;

(ii) under any written law; or

(iii) by a court, arbitral institution or mediation centre; or

(j) any request –

- (i) that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
- (ii) if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;
- (iii) for information that does not exist or cannot be found;
- (iv) for information that is trivial; or
- (v) that is otherwise frivolous or vexatious.

2. For the purposes of paragraph 1(j)(i), the organisation may have regard to the number and frequency of requests received.

SCHEDULE 4

(section 19(7))

EXCEPTIONS FROM CORRECTION REQUIREMENT

Section 19 does not apply in respect of —

- (a)* opinion data kept solely for an evaluative purpose;
- (b)* any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;
- (c)* the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;
- (d)* personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; or
- (e)* a document related to a prosecution if all proceedings related to the prosecution have not been completed.

SCHEDULE 5
(section 33(4))

SPECIFIED PURPOSES

1. Testing the effectiveness of the anonymisation of personal data in the possession or under the control of an organisation or a public agency.
2. Testing the integrity and confidentiality of anonymised information in the possession or under the control of an organisation or a public agency.
3. Assessing, testing or evaluating the systems and processes of an organisation or a public agency for ensuring or safeguarding the integrity and confidentiality of anonymised information –
 - (a) in the possession or under the control of the organisation or public agency; or
 - (b) transmitted or received by the organisation or public agency.

SCHEDULE 6

(section 41(3))

**CONSTITUTION AND PROCEEDINGS OF APPEAL PANEL
AND APPEAL COMMITTEE**

Appeal Panel

1. (1) Members of the Appeal Panel shall be appointed for such period as the Minister may determine and shall be eligible for re-appointment.

(2) The Minister may at any time revoke the appointment of any member of the Appeal Panel without assigning any reason.

(3) A member of the Appeal Panel may resign by giving notice in writing to the Minister.

Chairman of Appeal Panel or temporary Chairman of Appeal Panel

2. (1) The Chairman of the Appeal Panel shall be a person who is qualified to be a Judge of the Supreme Court.

(2) The Chairman of the Appeal Panel, unless his appointment is revoked by the Minister or he resigns during his term of office, shall hold office for such period as the Minister may determine and shall be eligible for re-appointment.

(3) The Minister may appoint any member to be a temporary Chairman of the Appeal Panel during the temporary incapacity from illness or otherwise, or during the temporary absence from Brunei Darussalam, of the Chairman.

Secretary to Appeal Panel

3. (1) There shall be a secretary to the Appeal Panel, appointed by the Minister, to provide administrative and secretarial support to the Chairman of the Appeal Panel, the Appeal Panel and every Appeal Committee, in the discharge of their functions, duties and powers under this Order.

(2) The secretary is to act in accordance with the instructions of the Chairman and, in particular, be responsible for —

(a) the acceptance, transmission, service and custody of documents relating to the Appeal Panel, Appeal Committees and proceedings relating to appeals; and

(b) keeping the records of proceedings relating to appeals in such form as the Chairman may direct.

(3) The secretary and any person authorised under sub-paragraph (4) may attend any meeting of an Appeal Committee to carry out their functions under this Order.

(4) The secretary may be assisted in carrying out the secretary's functions under this Order by persons authorised by the secretary.

Appeal Committee

4. (1) For the proper functioning of any Appeal Committee, the Chairman of the Appeal Panel may at any time —

(a) terminate the nomination of any member of the Appeal Committee; and

(b) reconstitute the Appeal Committee on the termination of the nomination, the expiry of the term of appointment or the withdrawal of any member of the Appeal Committee.

(2) The reconstitution of an Appeal Committee under sub-paragraph (1)(b) does not affect the validity of anything done by the Appeal Committee under this Order before, on or after the reconstitution of the Appeal Committee.

Proceedings of Appeal Committee

5. (1) The presiding member of an Appeal Committee is —

(a) the Chairman of the Appeal Panel, if he nominates himself as a member of the Appeal Committee; or

(b) the member of the Appeal Panel appointed by the Chairman as the presiding member of that Appeal Committee.

(2) In the absence at any meeting of the presiding member of an Appeal Committee referred to in sub-paragraph (1), another member of the Appeal Committee chosen by the members of that Appeal Committee present is to preside at that meeting.

(3) All matters coming before an Appeal Committee are to be decided by a majority of votes of those members present and, in the event of an equality of votes, the presiding member has a second or casting vote.

(4) Any member of the Appeal Panel whose term of appointment expires in the course of proceedings by an Appeal Committee to which he is appointed continues as a member of that Appeal Committee until the Appeal Committee —

(a) completes its work on the appeal; or

(b) is earlier reconstituted under paragraph 4(1)(b) without that member.

(5) An Appeal Committee is to meet for any purpose under this Order at such times and places as determined by the presiding member before the meeting.

Powers of Appeal Committee

6. (1) An Appeal Committee has all the powers and duties of the Authority that are necessary to perform its functions and discharge its duties under this Order.

(2) An Appeal Committee has the powers, rights and privileges vested in a court on the hearing of an action, including –

(a) the enforcement of the attendance of witnesses and their examination on oath or otherwise;

(b) the compelling of the production of documents; and

(c) the award of such costs or expenses as may be prescribed under section 65.

(3) A summons signed by such member of an Appeal Committee as may be authorised by the Appeal Committee is equivalent to any formal procedure capable of being issued in an action for enforcing the attendance of witnesses and compelling the production of documents.

(4) Where any person being duly summoned to attend before an Appeal Committee does not so attend, that person is guilty of an offence and liable on conviction to a fine not exceeding \$5,000, imprisonment for a term not exceeding 6 months or both.

(5) A witness before an Appeal Committee is entitled to the same immunities and privileges as if he were a witness before a court.

(6) All appeals shall be determined, having regard to the nature and complexity of the appeal, as soon as reasonably practicable.

(7) An Appeal Committee shall inform the Authority and the parties to the appeal of the date on and the place at which the appeal is heard.

(8) An Appeal Committee shall inform the Authority and the parties to the appeal of its decision in respect of the appeal and the reasons for its decision.

(9) Subject to other provisions of this Order and regulations made under this Order, an Appeal Committee may regulate its own procedure.

Allowances

7. Members of the Appeal Committee may receive a remuneration and travelling and subsistence allowances as the Minister may determine.

Validity of act or proceeding

8. No proceedings relating to an appeal before an Appeal Committee, and no act of the Chairman of the Appeal Panel or of the presiding member of an Appeal Committee, is to be nullified only because of –

(a) in the case of an appeal or proceeding before or act of an Appeal Committee, any vacancy in, or defect in the constitution of, the Appeal Committee; or

(b) any defect in the appointment of the Chairman of the Appeal Panel or any member (or presiding member) of an Appeal Committee.

Interpretation

9. In this Schedule, "appeal" means an appeal under section 42.

Made this 8th. day of Rejab, 1446 Hijriah corresponding to the 8th. day of January, 2025 at Our Istana Nurul Iman, Bandar Seri Begawan, Brunei Darussalam.

**HIS MAJESTY
THE SULTAN AND YANG DI-PERTUAN,
BRUNEI DARUSSALAM**