

THE DATA PROTECTION BILL, 2014

MEMORANDUM OF OBJECTS AND REASONS

This Bill seeks to introduce for the first time in the Cayman Islands legislation on data protection. Data protection is aimed principally at giving effect to the rights to privacy in relation to personal data while ensuring that certain exceptions are allowed. In preparing the Bill, consideration has been given, among other things, to section 9 of the Constitution of the Cayman Islands relating to private and family life.

**PART 1 - INTERPRETATION, PRINCIPLES, APPLICATION,
OBLIGATIONS AND OFFICE**

Clause 1 provides the short title and how the legislation will be brought into force.

Clause 2 contains the main definitions. Some of the key concepts defined there are “personal data”, “data controller”, “data processor”, “data subject” and “processing”.

Clause 3 contains another key definition, that of “sensitive personal data”, while clause 4 defines “special purposes”.

Clause 5, in conjunction with the schedules stated there, defines “data protection principles”.

Clause 6 states to whom this legislation applies. It applies to a data controller who is established in the Islands if the data are processed in the context of that establishment. It also applies to a data controller who is not established in the Islands but processes data in the Islands otherwise than for purposes of transit through the Islands. Where a data controller is not established in the Islands, he is required to nominate someone who is established in the Islands to represent him.

Clause 7, as read with the definition of “Commissioner” contained in clause 2, establishes the Information Commissioner appointed under the Information Commissioner Law (Law 10 of 2007) as the authority responsible for this legislation.

PART 2 - RIGHTS AND RESPONSIBILITIES OF DATA SUBJECTS AND OTHERS

Clause 8 provides for the general right of access to data. Subject to some exceptions and conditions, a data controller is obligated to supply certain information to a data subject where that information relates to the data subject.

Where the information cannot be supplied without revealing information relating to another data subject who can be identified from that information, clause 8(6) provides that the data controller is not obliged to comply with the request unless: (a) the other data subject has consented to the disclosure of the information to the person making the request; or (b) it is reasonable in all the circumstances to comply with the request without the consent of the other data subject.

Clause 8(10) makes provision regarding time limits for complying with a request for information. Where the Commissioner is satisfied that a data controller, in failing to supply information, has contravened the legislation, clause 8(11) provides that the Commissioner may issue an enforcement order under clause 50. This right to issue enforcement orders applies throughout the legislation in cases where a data controller fails to do or not to do anything which is required by the law to be done or not to be done.

Clause 9 deals with how requests are treated. This covers issues such as: the form in which requests are complied with; the subsequent or similar requests; and trade secrets.

Clause 10 gives certain rights to a data subject to stop the processing of data if processing occurs in certain circumstances.

Clause 11 allows a data subject to request that a data controller not use information relating to him for purposes of “direct marketing” which is defined in that clause.

Clause 12 limits the extent to which personal data that are processed by automatic means may be used to support a decision that “significantly affects the data subject”.

Clause 13 confers a right of a data subject to obtain compensation where he has suffered damage due to a contravention of this legislation.

Clause 14 empowers the Commissioner to order that a range of corrective measures be taken where data are inaccurate.

PART 3 - NOTIFICATIONS AND REGULATIONS

Clause 15 makes it obligatory for all persons who process personal data to be registered as data controllers.

Clause 16 specifies the particulars that must be notified by data controllers at registration.

Clauses 17 to 22 deal with other matters relating to notification by data controllers.

PART 4 - EXEMPTIONS

This Part contains the exemptions to certain general rules established in the legislation relating to data protection. The exemptions are based not just on the classification of the data but also other criteria. Some of the significant exemptions relate to crime and government fees and duties (clause 25), journalism, literature and art (clause 27), legal proceedings (clause 30), corporate finance (clause 33) and legal professional privilege (clause 35).

Clause 36 empowers the Cabinet, by regulations, to make additional exemptions.

PART 5 - FUNCTIONS OF INFORMATION COMMISSIONER

Clause 37 states that the Commissioner is independent and will not be subject to the direction or control of any other person or authority. It also empowers the Commissioner to appoint support staff.

Clause 38 provides that except as otherwise stated in this Law, the Commissioner is subject to the Public Service Management Law (2011 Revision).

Clause 39 sets out the general functions of the Commissioner. Different provisions in the legislation provide for more specific powers.

Clause 40 provides that a document that appears to have been signed by or on behalf of the Commissioner shall be presumed to have been so signed and be admissible in any proceedings unless the contrary is shown. This is intended to ensure that the Commissioner is not called every time to introduce the document, as the normal rules of evidence would require.

Clause 41 requires the Commissioner to prepare annual reports for the Legislative Assembly as well as prepare a budget.

Clause 42 establishes the Commissioner as the designated authority in the Islands for purposes of international cooperation relating to data protection.

Clauses 43 to 46 make certain administrative provisions relating to the Commissioner.

Clause 47 provides for the power of the Commissioner to issue codes of practice.

Clause 48 allows for complaints to the Commissioner.

Clause 49 empowers the Commissioner to require any person to provide him with all such information as he considers appropriate.

Clause 50 empowers the Commissioner to issue enforcement orders on a data controller where there are reasonable grounds to believe that a data controller has contravened, is contravening or is likely to contravene any provision of the legislation.

Clause 52 confers a right to seek judicial review where a person has received an information requirement, enforcement order or monetary penalty order under the legislation. Judicial review has to be sought within forty-five days.

Clause 56 empowers the Commissioner, upon being granted a warrant by a judge, to enter, search and obtain information relating to the exercise of his functions.

Clause 60 empowers the Commissioner to impose monetary penalties.

Clauses 62 to 63 contain provisions relating to offences.

PART 6 - ENFORCEMENT

Part 6 also deals with the mechanics of enforcement, the right of judicial review from decisions of the Commissioner to the Grand Court as well as related matters.

PART 7 - GENERAL

Part 7 deals with a number of diverse provisions. It also provides in clause 66 for a general power of the Cabinet to make regulations.

THE DATA PROTECTION BILL, 2014

ARRANGEMENT OF CLAUSES

**PART 1 - INTERPRETATION, PRINCIPLES, APPLICATION,
OBLIGATIONS AND OFFICE**

1. Short title and commencement
2. Interpretation
3. Sensitive personal data
4. Special purposes
5. The data protection principles: their content, regulations about them, and duty to comply with them
6. Application of Law: duty of data controller outside the Islands to nominate a Cayman Islands representative
7. Information Commissioner

**PART 2 - RIGHTS AND RESPONSIBILITIES OF DATA SUBJECTS AND
OTHERS**

8. Fundamental rights of access to personal data
9. Treatment of requests under section 8
10. Right to stop processing
11. Right to stop processing for direct marketing
12. Rights in relation to automated decision-making
13. Compensation for failure to comply
14. Rectification, blocking, erasure and destruction

PART 3 - NOTIFICATIONS BY DATA CONTROLLERS

15. No processing without registration
16. Notification by data controllers
17. Register of notifications
18. Duty to notify changes
19. Offences and penalties
20. Preliminary determination by Commissioner as to restricted processing
21. Duty of certain data controllers to make certain information available
22. Personal data breaches

PART 4 - EXEMPTIONS

23. Effect of this Part
24. National security
25. Crime, government fees and duties
26. Health, education or social work
27. Journalism, literature or art
28. Research, history or statistics
29. Information available to public by or under enactments
30. Legal proceedings
31. Personal, family or household affairs
32. Honours
33. Corporate finance
34. Negotiations
35. Legal professional privilege
36. Exemptions by regulations

PART 5 - FUNCTIONS OF INFORMATION COMMISSIONER

37. Independence and powers
38. Commissioner to be subject to Public Service Management Law (2007 Revision)
39. General functions of Commissioner
40. Documents signed by the Commissioner
41. Reports to Legislative Assembly and budget
42. International cooperation
43. Protection of Commissioner
44. Defamation
45. Consultation of Commissioner
46. Promotion of the Law by Commissioner
47. Codes of practice

PART 6 - ENFORCEMENT

48. Complaints
49. Information orders
50. Enforcement orders
51. Failure to comply with order
52. Right to judicial review
53. Failure to judicially review a requirement or order
54. Disclosure of information
55. Confidentiality of information

- 56. Entry and search of premises, obtaining of information
- 57. Warrant not exercisable
- 58. Offences in respect of warrants
- 59. Unlawful obtaining etc. of personal data
- 60. Power of the Commissioner to impose monetary penalty
- 61. Guidance about monetary penalty orders
- 62. General provisions relating to offences
- 63. Liability for offences

PART 7 - GENERAL

- 64. Law binds Crown
- 65. Service of orders, etc
- 66. Regulations

SCHEDULE 1: DATA PROTECTION PRINCIPLES AND THEIR INTERPRETATION

SCHEDULE 2: FIRST PRINCIPLE - CONDITIONS FOR PROCESSING OF ANY PERSONAL DATA

SCHEDULE 3: FIRST PRINCIPLE - CONDITIONS FOR PROCESSING OF SENSITIVE PERSONAL DATA

SCHEDULE 4: TRANSFERS TO WHICH EIGHTH PRINCIPLE DOES NOT APPLY

SCHEDULE 5: CONDITIONS OF CONSENT

CAYMAN ISLANDS

**A BILL FOR A LAW TO PROVIDE FOR THE PROTECTION OF
PERSONAL DATA; AND FOR INCIDENTAL AND CONNECTED
PURPOSES**

ENACTED by the Legislature of the Cayman Islands.

**PART 1 - INTERPRETATION, PRINCIPLES, APPLICATION AND
OBLIGATIONS AND OFFICE**

1. (1) This Law may be cited as the Data Protection Bill, 2014. Short title and
commencement

(2) This Law shall come into force on such date as may be appointed by Order made by the Cabinet, and different dates may be appointed for different provisions of this Law and in relation to different matters.

2. In this Law - Interpretation

“business” includes any trade or profession;

“Commissioner” means the Information Commissioner appointed under section 35 of the Freedom of Information Law, 2007; (Law 10 of 2007)

“consent” means any freely given specific, informed and explicit indication of a data subject's wishes by which he, either by a statement or by a clear act, signifies

his agreement to personal data relating to him being processed and, in determining consent, Schedule 5 shall apply;

“data controller” means the person who, alone or jointly with others, determines the purposes, conditions and means of the processing of personal data and includes a representative referred to in section 6(2);

“data processor” means any person who processes personal data on behalf of a data controller, but for the avoidance of doubt does not include an employee of the data controller;

“data protection principles” has the meaning referred to in section 5;

“data subject” means -

- (a) an identified living individual; or
- (b) a living individual who can be identified directly or indirectly by means reasonably likely to be used by the data controller or by any other person.-

“enforcement order” means an order under section 50;

(2005 Revision) “health professional” means an individual registered to practise under any of the professions specified in the Health Practice Law (2005 Revision) or any other law relating to health;

“health record” means a record that -

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

“inaccurate”, in relation to personal data, includes data that are misleading, incomplete or out of date;

“non-disclosure provisions” means the following provisions to the extent that they are inconsistent with the disclosure in question -

- (a) the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3;
- (b) the second and third data protection principles; and
- (c) sections 10 and 14;

“person” includes any corporation, either aggregate or sole, and any club, society, association, public authority or other body, of one or more persons;

“personal data” means data relating to a data subject and includes such data as -

- (a) the data subject's location data, his online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the data subject;
- (b) an expression of opinion about the data subject; or
- (c) any indication of the intentions of the data controller or any other person in respect of the data subject;

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

“processing” means obtaining, recording or holding the data, or carrying out any operation or set of operations on personal data, including -

- (a) organizing, adapting or altering the information or data;
- (b) retrieving, consulting or using the information or data;
- (c) disclosing the information or data by transmission, dissemination or otherwise making it available; or
- (d) aligning, combining, blocking, erasing or destroying the information or data;

“public authority” means -

- (a) a ministry, portfolio or department;
- (b) a statutory body or authority, whether incorporated or not;
- (c) a company which -
 - (i) is wholly owned by the Government or in which the Government has a direct or indirect controlling interest;
 - (ii) is specified in an Order made by the Cabinet;
- (d) any other body or organisation specified by the Cabinet by Order on account of providing services of a public nature which are essential to the welfare of Caymanian society;

“public register” means any register that, pursuant to a requirement imposed under an enactment or in pursuance of an international agreement, is open to public inspection or open to inspection by any person having a legitimate interest in the subject matter of the register;

“publish”, in relation to journalistic, literary or artistic material, means to make available to the public or any section of the public;

“recipient”, in relation to any personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the relevant

data controller, a relevant data processor, or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law;

“register” means the register maintained under section 17;

(2010 Revision)

“registered company” means a company within the meaning of section 2 of the Companies Law (2013 Revision);

“regulations” means regulations made under this Law;

“restricted processing” has the meaning assigned in section 20;

“sensitive personal data” has the meaning assigned in section 3;

“special purposes” has the meaning assigned in section 4;

“staff”, in relation to the Commissioner, includes any individual employed in the office of the Commissioner;

“subject information provisions” means -

- (a) the first data protection principle to the extent to which it requires compliance with paragraph 2 of Part 2 of Schedule 1; and
- (b) section 8; and

“third party”, in relation to personal data, means any person other than -

- (a) the data subject;
- (b) the data controller; or
- (c) any data processor or other person authorized to process data for the data controller or processor.

Sensitive personal data

3. In this Law, “sensitive personal data” means, in relation to a data subject, personal data consisting of -

- (a) the racial or ethnic origin of the data subject;
- (b) the political opinions of the data subject;
- (c) the data subject’s religious beliefs or other beliefs of a similar nature;
- (d) whether the data subject is a member of a trade union;
- (e) genetic data;
- (f) the data subject’s physical or mental health or condition;

- (g) the data subject's sex life;
- (h) the data subject's commission, or alleged commission, including by way of arrest or charging, of any offence; or
- (i) any proceedings for any offence committed, or alleged, including by way of arrest or charging, to have been committed, by the data subject, the disposal of any such proceedings or any sentence of a court in the Islands or elsewhere.

4. In this Law, "special purposes" means any one or more of the following - Special purposes

- (a) the purposes of journalism;
- (b) artistic purposes;
- (c) literary purposes.

5. (1) References in this Law to the data protection principles are to the principles set out in Part 1 of Schedule 1. The data protection principles: their content, regulations about them, and duty to comply with them

(2) The data protection principles shall be interpreted in accordance with Part 2 of Schedule 1.

(3) Schedules 1, 2, 3, 4 and 5 shall apply.

(4) Subject to section 23, a data controller shall comply with the data protection principles in relation to personal data with respect to which he is a data controller.

6. (1) This Law applies to a data controller in respect of any personal data only if - Application of Law; duty of data controller outside the Islands to nominate a Cayman Islands representative

- (a) the data controller is established in the Islands and the personal data are processed in the context of that establishment; or
- (b) the data controller is not established in the Islands but the personal data are processed in the Islands otherwise than for the purposes of transit through the Islands.

(2) A data controller referred to in subsection (1)(b) shall nominate for the purposes of this Law a local representative resident in the Islands who shall for all purposes within the Islands be the data controller and, without limiting the generality of this provision, bear all obligations under this Law as if he were the data controller.

(3) For the purposes of subsections (1) and (2), each of the following is to be treated as established in the Islands -

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

- (b) a body incorporated or registered as a foreign company under the law of the Islands;
- (c) a partnership or other unincorporated association formed under the law of the Islands; or
- (d) any person who does not fall within paragraph (a), (b) or (c) but maintains in the Islands -
 - (i) an office, branch or agency through which the person carries on any activity, or
 - (ii) a regular practice.

Information
Commissioner

(Law 10 of 2007)

7. The provisions of the Freedom of Information Law, 2007 relating to appointment, tenure and office of the Information Commissioner shall have effect.

PART 2 - RIGHTS AND RESPONSIBILITIES OF DATA SUBJECTS AND OTHERS

Fundamental rights of
access to personal data

8. (1) A data subject is entitled to be informed by a data controller whether the personal data of which he is the data subject are being processed by or on behalf of that data controller, and, if that is the case, to be given by that data controller a description of -

- (a) the data subject's personal data;
- (b) the purposes for which they are being or are to be processed by or on behalf of that data controller; and
- (c) the recipients or classes of recipients to whom they are or may be disclosed by or on behalf of that data controller.

(2) A data subject is entitled to the communication in intelligible form, by the relevant data controller, of -

- (a) the data subject's personal data; and
- (b) any information available to the relevant data controller as to the source of those personal data.

(3) If the processing by automatic means of the data subject's personal data for the purpose of evaluating matters relating to the data subject, including the data subject's performance at work, creditworthiness, reliability or conduct, has constituted or is likely to constitute the sole basis for any decision significantly affecting the data subject, the data subject is entitled to be informed by the relevant data controller of the logic for that decision.

(4) A data controller is not obliged under subsection (1), (2) or (3) to supply any personal data unless he has received -

- (a) a request in writing; and

- (b) such fee, not exceeding a maximum that may be prescribed by regulations made by Cabinet, as the data controller may require.

(5) If a data controller reasonably requires further information in order to be satisfied as to the identity of the data subject making the request or to locate the information that the data subject seeks, and has informed the data subject in writing of the requirement, the data controller is not obliged to comply with the request unless supplied with that information, during which the time specified in subsection (6) shall automatically stand suspended.

(6) A data controller shall comply with a request under this section within thirty calendar days (or such other period as may be prescribed by regulations made by Cabinet) of the date on which he is in possession of both the request and fee referred to in subsection (4), but where the data controller has requested further information under subsection (5), the period shall not resume until the information has been supplied.

(6) If a data controller cannot comply with the request without disclosing personal data relating to another data subject who can be identified from that personal data, the data controller is not obliged to comply with the request unless -

- (a) the other data subject has consented to the disclosure of the personal data to the person making the request; or
- (b) it is reasonable in all the circumstances to comply with the request without the consent of the other data subject.

(7) In subsection (6), the reference to personal data relating to another data subject includes a reference to personal data identifying that data subject as the source of the personal data sought in the request.

(8) Subsection (6) shall not be construed as excusing a data controller from communicating so much of the personal data sought in the request as can be communicated without disclosing the identity of the other data subject concerned, whether by the omission of names or other identifying particulars or otherwise.

(9) In determining for the purposes of subsection (6)(b) whether it is reasonable in all the circumstances to comply with the request without the consent of the other data subject concerned, the data controller shall have regard to, in particular -

- (a) any duty of confidentiality owed to the other data subject;
- (b) any steps taken by the data controller to seek the consent of the other data subject;
- (c) whether the other subject is capable of giving consent; and

(d) any express refusal of consent by the other data subject.

(11) If the Commissioner is satisfied on the application of a data subject who has made a request under this section that a data controller has contravened this section in failing to comply with the request, the Commissioner shall issue an enforcement order under section 50 ordering the data controller to comply with the request.

(12) If personal data are being processed by or on behalf of a data controller who receives a request under this section from a data subject who is the data subject of those data, the obligation to supply the personal data under this section includes an obligation to give the data subject a statement of the data subject's rights under this Law in such form, and to such extent, as may be prescribed by regulations made by Cabinet.

Treatment of requests
under section 8

9. (1) The obligation imposed by section 8(2)(a) shall be complied with by supplying the data subject with a copy of the personal data in the format requested unless -

- (a) the supply of such a copy is not possible or would involve disproportionate effort; or
- (b) the data subject agrees otherwise.

(2) If any of the personal data referred to in section 8(2)(a) are expressed in terms that are not intelligible without explanation the copy shall be accompanied by an adequate explanation.

(3) If a data controller has previously complied with a request under section 8 by the data subject referred to therein, the data controller is not obliged to comply with a subsequent identical or similar request under that section by the data subject unless the interval between compliance with the previous request and the making of the current request is reasonable.

(4) In determining whether the interval referred to in subsection (3) is reasonable, regard shall be had to the nature of the personal data, the purpose for which the personal data are processed and the frequency with which the personal data are altered.

(5) Section 8(3) shall not be regarded as requiring the provision of information as to the logic of any decision to the extent that the information constitutes a trade secret.

(6) Personal data and other information supplied under section 8 shall be supplied by reference to the data in question at the time when the request for the

personal data is received, except that account may be taken of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request.

10. (1) A data subject is entitled at any time by notice in writing to a data controller to require the data controller to cease, or not to begin, processing, or processing for a specified purpose or in a specified manner, the data subject's personal data.

Right to stop processing

(2) The data controller shall, as soon as practicable but in any case within twenty-one calendar days of receiving a notice under subsection (1), comply with that notice unless -

- (a) the processing is necessary for the performance of a contract to which the data subject is a party or the taking of steps at the request of the data subject with a view to entering into a contract;
- (b) the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
- (c) the processing is necessary in order to protect the vital interests of the data subject; or
- (d) in such other cases as may be prescribed by regulations made by the Cabinet,

and state to the data subject the reasons for his non-compliance with the notice.

(3) If, on the application of any data subject who has given notice under subsection (1), the Commissioner is satisfied that the data controller in question has failed to comply with the notice, the Commissioner may issue an enforcement order under section 50.

(4) The failure by a data subject to exercise the right conferred by subsection (1) does not affect any other right conferred on the data subject by this Law.

11. (1) In this section, "direct marketing" means the communication, by whatever means, of any advertising, marketing, promotional or similar material, that is directed to one or more individuals.

Right to stop processing
for direct marketing

(2) A data subject is entitled at any time by notice in writing to a data controller to require the data controller at the end of such period as is reasonable in the circumstances to cease, or not to begin, processing for the purposes of direct marketing personal data relating to the data subject.

(3) If, on the application of any data subject who has given notice under subsection (1), the Commissioner is satisfied that the data controller in question has failed to comply with the notice, the Commissioner may issue an enforcement order under section 50.

(4) The failure by a data subject to exercise the right conferred by subsection (2) does not affect any other right conferred on the data subject by this Law.

Rights in relation to
automated decision-
making

12. (1) A data subject is entitled at any time, by notice in writing to a data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller that significantly affects the data subject is based solely on the processing by automatic means of his personal data for the purpose of evaluating matters relating to the data subject including the data subject's performance at work, creditworthiness, reliability or conduct.

(2) If no notice has been given under subsection (1) and a decision that significantly affects a data subject is based solely on processing specified in that subsection -

- (a) the data controller shall as soon as reasonably practicable notify the data subject that the decision was taken on that basis; and
- (b) the data subject is entitled, within twenty-one calendar days after receiving that notification from the data controller, by notice in writing, to require the data controller to reconsider the decision or to take a new decision otherwise than on that basis.

(3) The data controller shall, within twenty-one calendar days after receiving a notice under subsection (2)(b), give the data subject a written notice specifying the steps that the data controller intends to take to comply with the notice.

(4) A notice under subsection (1) does not have effect in relation to, and nothing in subsection (2) applies to, a decision -

- (a) in respect of which one condition in each of subsections (5) and (6) is satisfied; or
- (b) that is made in such other circumstances as may be prescribed by regulations made by Cabinet.

(5) The first condition is that the decision -

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

- (ii) with a view to entering into such a contract; or
 - (iii) in the course of performing such a contract; or
 - (b) is authorized or required by or under any enactment.
- (6) The second condition is that -
- (a) the effect of the decision is to grant a request of the data subject; or
 - (b) steps have been taken to safeguard the legitimate interests of the data subject including by allowing the data subject to make representations.

(7) If the Commissioner is satisfied on the application of a data subject that a person taking a decision in respect of the data subject has failed to comply with a notice under subsection (1) or (2)(b), the Commissioner may among other things issue an enforcement order ordering the data controller to reconsider the decision where that decision is not based solely on the processing mentioned in subsection (1).

13. A person who suffers damage by reason of any contravention by a data controller of any requirement of this Law has a cause of action for compensation from the data controller for that damage.

Compensation for failure to comply

14. (1) If the Commissioner is satisfied on a complaint made under section 48 that personal data are inaccurate, the Commissioner may order the data controller to rectify, block, erase or destroy -

Rectification, blocking, erasure or destruction

- (a) those data; and
- (b) any other personal data in respect of which the person is the data controller and that contain an expression of opinion that appears to the Commissioner to be based on the inaccurate data.

(2) Subsection (1) applies whether or not the personal data accurately record information received or obtained by the data controller from the data subject or a third party, but if the data accurately record such information then the Commissioner may instead of making an order under subsection (1) -

- (a) make an order requiring the personal data to be supplemented by a statement of the facts relating to the matters dealt with by the data as the Commissioner may approve;
- (b) make such order as he thinks fit to ensure the accuracy of the data, having regard to the purpose or purposes for which the data were obtained and further processed, with or without a further order requiring the data to be supplemented by a statement of the facts relating to the matters dealt with by the data as the Commissioner may approve; or

- (c) make an order requiring the data controller to ensure that the data indicate that in the data subject's view the data are inaccurate.

(3) If the Commissioner -

- (a) makes an order under subsection (1); or
- (b) is satisfied on a complaint made under section 48 that personal data that have been rectified, blocked, erased or destroyed were inaccurate,

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

(4) If the Commissioner is satisfied on the application of a data subject -

- (a) that the data subject has suffered damage by reason of a contravention by a data controller of any of the requirements of, or under, this Law in respect of the data subject's personal data, in circumstances entitling the individual to compensation under section 13; and
- (b) that there is a substantial risk of further contravention in respect of those data in such circumstances,

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

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

(6) In determining whether it is reasonably practicable to require notification under subsection (3) or (5), the Commissioner shall have regard, in particular, to the number of individuals who would have to be notified

PART 3 - NOTIFICATIONS BY DATA CONTROLLERS

No processing without registration

15. (1) Unless otherwise provided for in this Law, no person may process personal data unless the data controller of that personal data is included in the register referred to in section 17(1).

(2) If it appears to Cabinet that processing of a particular description is unlikely to prejudice the rights and freedoms of data subjects, the Cabinet may by

regulations prescribe processing, in all cases or in specified cases, of that description as processing to which subsection (1) shall not apply.

(3) The Cabinet may make regulations relating to the operation of this section.

16. (1) A data controller who seeks registration shall notify the Commissioner of -

Notification by data controllers

- (a) the name and address of the data controller;
- (b) a description of the personal data being, or to be, processed by or on behalf of the data controller and of the category or categories of data subject to which they relate;
- (c) a description of the purpose or purposes for which the data are being or are to be processed;
- (d) a description of the recipients, if any, to whom the data controller intends or may wish to disclose the data;
- (e) the names, or a description, of any countries or territories outside the Islands to which, directly or indirectly, the data controller transfers, or intends or may wish to transfer, the data;
- (f) if personal data are being, or are intended to be, processed by a data controller in circumstances in which the prohibition in section 15(1) is excluded by section 15(2) or (3) and a notification in respect of the data controller under section 18 does not extend to those data, a statement of that fact;
- (g) a general description of measures to be taken for the purpose of complying with the seventh data protection principle; and
- (i) such other information as the Commissioner may require.

(2) For purposes of this Part, so far as it relates to the addresses of data controllers -

- (a) the address of a registered company is that of its registered office; and
- (b) the address of an individual carrying on a business is that of the individual's principal place of business in the Islands.

17. (1) The Commissioner shall maintain a register of persons who have notified him under section 16 and such register may be in electronic form.

Register of notifications

(2) Each entry in the register shall consist of -

- (a) the registerable particulars notified under section 16 or those particulars as amended under section 18(3); and

(b) such other information as the Commissioner may consider appropriate.

(3) The Commissioner -

(a) shall make the register available for inspection, in visible and legible form, by members of the public at reasonable hours and free of charge; and

(b) may provide such facilities for making that information available to the public free of charge as he considers appropriate.

(4) The Commissioner shall, on application, supply any person with a certificate signed by him or on his behalf indicating the particulars contained in the register.

Duty to notify changes

18. (1) A data controller shall notify the Commissioner, in such circumstances, at such times and in such a form as the Commissioner may require, if the particulars referred to in section 16(1) or regulations promulgated under section 15 no longer reflect the current particulars and measures for that data controller.

(2) The data controller shall notify the Commissioner of the changes that would allow the notified registerable particulars and regulations promulgated under section 15 to reflect what is current as soon as practicable and, in any event, within a period of twenty-eight calendar days from the date when those particulars or measures no longer reflect what is current.

(3) The Commissioner shall amend the relevant entry in the register as soon as practicable after being notified by a data controller under subsection (1).

Offences

19. A person who contravenes section 15(1) or section 18(1) or (2) commits an offence.

Preliminary determination by Commissioner as to restricted processing

20. The Cabinet may, upon the recommendation of the Commissioner, make regulations governing types of processing requiring the prior approval of the Commissioner, being processing that is considered particularly likely to -

(a) cause substantial damage or substantial distress to data subjects; or

(b) otherwise significantly prejudice the rights and freedoms of data subjects.

Duty of certain data controllers to make certain information available

21. (1) If personal data are processed in a case where -

(a) because of section 15(2) or (3), section 15(1) does not apply to the processing; and

- (b) the relevant data controller has not notified the registerable particulars in section 16(1) in respect of that processing,

the data controller shall, nonetheless, within twenty-one days after receiving a written request from any person, make those particulars available to that person in writing free of charge.

(2) The Cabinet may, by regulations, make provision for exemptions from the operation of this section, and this section has effect subject to any such exemptions.

(3) A data controller who fails to comply with the duty imposed by subsection (1) commits an offence.

22. (1) In the case of a personal data breach, the data controller shall, without undue delay, but no longer than five calendar days after he should, with the exercise of reasonable diligence, have been aware of that breach, notify that personal data breach to the data subject of the data in question and to the Commissioner, describing -

Personal data breaches

- (a) the nature of the breach;
- (b) the consequences of the breach;
- (c) the measures proposed or taken by the data controller to address the breach; and
- (d) the measures recommended by the data controller to the data subject of the personal data in question to mitigate the possible adverse effects of the breach.

(2) A data controller who contravenes subsection (1) commits an offence and is liable to a fine of one hundred thousand dollars.

PART 4 - EXEMPTIONS

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

Effect of this Part

24. (1) Personal data are exempt from any of the provisions of -

- (a) the data protection principles; and
- (b) Parts 2, 3 and 6,

Exemption based on national security

if the exemption from all or any of the provisions is required for the purpose of safeguarding national security.

(2) The Governor may, for the purpose mentioned in subsection (1), issue a certificate with respect to any personal data exempting that data from all or any of the provisions referred to in that subsection and that certificate shall be sufficient evidence of that fact.

(3) The certificate issued under subsection (2) shall identify the personal data to which it applies.

(4) If in any consideration of a matter by the Commissioner it is claimed by a data controller that a certificate under this section applies to any personal data, any party may make an application to the Commissioner contending that the certificate does not apply to the personal data with respect to which the complaint is made.

(5) Notwithstanding subsection (4), unless the Commissioner makes a determination under subsection (6), the certificate shall be conclusively presumed so to apply.

(6) On an application under subsection (4), the Commissioner may determine that the certificate does not apply to the personal data with respect to which the complaint is made.

(7) A document purporting to be a certificate under this section and signed by the Governor shall be received in evidence and taken to be such a certificate unless the contrary is proved.

Exemption: crime,
government fees and
duties

25. (1) Personal data processed for any of the following purposes -

- (a) the prevention, detection or investigation of crime;
- (b) the apprehension or prosecution of persons who are suspected to have committed an offence anywhere; or
- (c) the assessment or collection of any fees or duty, or of any imposition of a similar nature, in the Islands,

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3), the non-disclosure provisions and section 8, to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters referred to in paragraph (a) to (c).

(2) Personal data that -

- (a) are processed for the purpose of discharging functions under any Law; and

- (b) consist of information obtained for such a purpose from a person who had it in his possession for any of the purposes referred to in subsection (1)(a) to (c),

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

26. (1) The Cabinet may, by regulations, exempt from the subject information provisions, or modify those provisions in relation to, personal data consisting of information as to the physical or mental health or condition of the data subject.

Exemption or modification for sake of health, education or social work

(2) The Cabinet may, by regulations, exempt from the subject information provisions, or modify those provisions, in relation to personal data in respect of which the data controller is the proprietor, governor, governing body, director or manager of, or a principal or teacher at, a school, and that consist of information relating to persons who are or have been pupils at the school.

(3) The Cabinet may by regulations, exempt from the subject information provisions, or modify those provisions in relation to, personal data of such other descriptions as may be specified in the regulations, being information -

- (a) processed by a public authority; and
- (b) appearing to the Cabinet to be processed in the course of, or for the purposes of, carrying out social work in relation to the data subject or other data subjects, to the extent that the Cabinet consider that the application to the data of those provisions, or of those provisions without modification, would be likely to prejudice the carrying out of social work.

27. (1) Personal data which are processed only for the special purposes are exempt from any provision to which this section relates if -

Exemption for sake of journalism, literature or art

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

(2) This section relates to the following provisions -

- (a) the data protection principles except the seventh data protection principle; and

(b) section 10.

(3) In considering for the purposes of subsection (1)(b) whether the belief of a data controller that publication would be in the public interest was or is a reasonable one, regard may be had to the data controller's compliance with any code of practice that is relevant to the publication in question.

Exemption for sake of research, history or statistics

28. (1) In this section -

“relevant conditions” means the conditions -

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

(2) Personal data processed for statistical purposes or for the purposes of historical or scientific research in compliance with the relevant conditions are exempt from the first data protection principle to the extent to which it requires compliance with subparagraph 1(b) of paragraph 2 of Part 2 of Schedule 1.

(3) Subsection (2) applies if -

- (a) the provision of such information proves impossible or would involve a disproportionate effort; or
- (b) processing is required by or under any enactment.

(4) For the purposes of the second data protection principle, the further processing of personal data for the purpose of research, history or statistics in compliance with the relevant conditions is not to be regarded as incompatible with the purposes for which they were obtained.

(5) Personal data processed solely for the purposes of scientific research or kept in a form that identifies a data subject for a period which does not exceed the period necessary for the sole purpose of creating statistics are exempt from section 8.

(6) Subsection (5) applies if -

- (a) the data are processed in compliance with the relevant conditions;
- (b) there is no risk of breaching the rights and freedoms of the data subject; and

- (c) the results of the research or any resulting statistics are not made available in a form that identifies one or more of the data subjects.

(7) Personal data processed for historical, statistical or scientific purposes in compliance with the relevant conditions are exempt from the fifth data protection principle to the extent to which compliance would be likely to prejudice those purposes.

29. Personal data are exempt from -

- (a) the subject information provisions;
- (b) the fourth data protection principle and section 14(1) to (3); and
- (c) the non-disclosure provisions,

Exemption for information available to public by or under enactment

if the data consist of information that the data controller is obliged by or under any enactment to make available to the public, including by inspection, gratuitously or on payment of a fee.

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

Disclosures required by law or made in connection with legal proceedings

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

- (a) for the purpose of, in connection with, or in contemplation of, any quasi-judicial or legal proceedings;
- (b) for the purpose of obtaining legal advice; or
- (c) otherwise for the purposes of establishing, exercising or defending a legal right.

31. Personal data processed by an individual only for the purposes of that individual's personal, family or household affairs are exempt from the data protection principles and Parts 2 and 3.

Exemption for data processed for personal, family or household affairs

32. Personal data are exempt from the subject information provisions if processed for the purposes of the conferring by the Crown or the Premier of any honour or dignity.

Exemption with respect to honours

33. (1) If personal data are processed for the purposes of, or in connection with, a corporate finance service provided by a relevant person -

Corporate finance

- (a) the data are exempt from the subject information provisions to the extent to which either -

- (i) the application of those provisions to the data could affect the price of any instrument already in existence or that is to be or may be created, or
 - (ii) the data controller reasonably believes that the application of those provisions to the data could affect the price of any such instrument; and
 - (b) to the extent that the data are not exempt from the subject information provisions by virtue of paragraph (a), they are exempt from those provisions if the exemption is required for the purpose of safeguarding an important economic or financial interest of the Islands.
- (2) For the purposes of subsection (1)(b) the Cabinet may by regulations specify -
- (a) matters to be taken into account in determining whether exemption from the subject information provisions is required for the purpose of safeguarding an important economic or financial interest of the Islands; or
 - (b) circumstances in which exemption from those provisions is, or is not, to be taken to be required for that purpose.
- (3) In this section -
- “corporate finance service” means a service consisting in -
- (a) underwriting in respect of issues of, or the placing of issues of, any instrument;
 - (b) advice to undertakings on capital structure, industrial strategy and related matters and advice and service relating to mergers and the purchase of undertakings; or
 - (c) services relating to such underwriting as is mentioned in paragraph (a);
- “instrument” means an instrument representing investment within the meaning of any Law in the Islands;
- “price” includes value;
- “relevant person” means -
- (a) a registered person within the meaning of any Law in respect of investment business within the meaning of that Law or a person who is exempted by that Law from the obligation to be registered under that Law in respect of such investment business;

- (b) a person who is an authorised person under such Law, or is an exempt person under that Law, in respect of such investment business;
- (c) a person who may be prescribed by regulations made by Cabinet for the purposes of this paragraph;
- (d) a person who, in the course of his employment, provides to his employer a service falling within paragraph (b) or (c) of the definition of “corporate finance service”; or
- (e) a partner who provides to other partners in the partnership a service falling within either of those paragraphs.

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

35. Personal data are exempt from the subject information provisions if the data consist of information in respect of which legal professional privilege applies. Legal professional privilege

36. (1) Subject to subsection (2), the Cabinet may, after consultation with the Commissioner, by regulations - Exemptions by regulations

- (a) exempt from subject information provisions personal data consisting of information, the disclosure of which is prohibited or restricted by or under any enactment; or
- (b) exempt from the non-disclosure provisions personal data consisting of information, the disclosure of which is made in circumstances specified in the regulations.

(2) The Cabinet shall not grant an exemption under subsection (1) unless it considers the exemption to be necessary for the purpose of safeguarding the interests of data subjects or the rights and freedoms of any other individual.

PART 5 - FUNCTIONS OF INFORMATION COMMISSIONER

37. (1) The Commissioner shall have all powers, direct and incidental, as are necessary or convenient to undertake his functions as provided for under this Law and for purposes of this subsection, the word “functions” includes power, authority and duty. Independence and powers

(2) In the exercise of his functions, the Commissioner shall be independent and not be subject to the direction or control of any other person or authority.

(3) The Commissioner may appoint such officers and employees as are necessary to enable him to perform his functions under this Law.

(4) The Commissioner shall, from moneys appropriated by the Legislative Assembly, meet operational expenses of his office and the provision of a reserve fund and, where there is any balance separate from the reserve fund, pay such balance into the general revenues of the Islands.

(5) The Cabinet may make additional provisions relating to the operation of the reserve fund.

Commissioner to be subject to Public Service Management Law (2007 Revision)

38. Except as otherwise stated in this Law or the Freedom of Information Law, 2007, the Commissioner shall be subject to the Public Service Management Law (2007 Revision).

General functions of Commissioner

39. The principal functions of the Commissioner include -

- (a) to hear, investigate and rule on complaints made under this Law;
- (b) to monitor, investigate and report on the compliance by data controllers with their obligations under this Law;
- (c) to intervene and deliver opinions and orders related to processing operations;
- (d) to order the rectification, blocking, erasure or destruction of data;
- (e) to impose a temporary or permanent ban on processing;
- (f) to make recommendations for reform both of a general nature and directed at specific data controllers;
- (g) to maintain the public register of data controllers and their processing operations under this Law;
- (h) to engage in proceedings where the provisions of this Law have been violated, or refer these violations to the appropriate authorities;
- (i) to cooperate with other data protection supervisory authorities;
- (j) to publicize and promote the requirements of this Law and the rights of data subjects under it; and
- (k) to do anything which appears to him to be incidental or conducive to the carrying out of his functions under this Law.

Documents signed by Commissioner

40. A document that appears to have been signed by or on behalf of the Commissioner shall be presumed to have been so signed and be admissible in any proceedings unless the contrary is shown.

Reports to Legislative Assembly and budget

41. The Commissioner shall, as soon as reasonably practicable after the end of each year, lay before the Legislative Assembly -

- (a) a report of the operation of this Law during the year and may from time to time submit such other reports as the Commissioner thinks appropriate; and
- (b) accounts audited under the Public Management and Finance Law (2013 Revision). (2013 Revision)
42. (1) The Commissioner is the designated authority in the Islands for the purposes of international cooperation related to data protection. International cooperation
- (2) The Commissioner shall also carry out any data protection functions under regulations made by the Cabinet to give effect to any international obligations.
43. Neither the Commissioner nor any member of staff of his office shall be liable in damages for anything done or omitted in the discharge or purported discharge of their respective functions under this Law unless it is shown that the act or omission was in bad faith. Protection of Commissioner
44. (1) It is a defence to any civil or criminal proceedings in libel or slander that information supplied to the Commissioner was communicated to the Commissioner pursuant to this Law. Defamation
- (2) It is a defence to any civil or criminal proceedings in libel or slander that information communicated by a data controller to any person under this Law was communicated in the first instance by a third person, unless the communication to or by the data controller was made maliciously.
45. A public authority that is drawing up administrative measures or rules relating to the protection of data subjects' rights and freedoms with regard to data processing shall consult the Commissioner on the content of such measures or rules. Consultation of Commissioner
46. (1) The Commissioner shall promote good practice and observance of this Law by data controllers. Promotion of the Law by Commissioner
- (2) The Commissioner may arrange for the dissemination of information about the operation of this Law, about good practice, and about other matters within the scope of his functions under this Law, and may give advice to any person as to any of those matters.
47. (1) The Cabinet may, after consulting with the Commissioner, make regulations for the preparation and dissemination of codes of practice which may be specific to a particular industry or processing operation. Codes of practice

(2) A direction under subsection (3) shall describe the personal data or processing to which the code of practice shall relate, and may also describe the persons or classes of persons to whom it shall relate.

(3) The Commissioner shall also -

- (a) if the Commissioner considers it appropriate to do so, encourage trade associations to prepare, and to disseminate to their members, codes of practice for guidance as to good practice; and
- (b) if a trade association submits a code of practice for the Commissioner's consideration, consider the code and, after such consultation with data subjects or persons representing data subjects as appears to the Commissioner to be appropriate, notify the trade association whether, in the Commissioner's opinion, the code promotes good practice.

(4) The Commissioner may, with the consent of the relevant data controller, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment.

(5) The Commissioner may charge such fees as he thinks fit for any services provided by him under this Law.

(6) In this section -

“good practice” means such practice in the processing of personal data as appears to the Commissioner to be desirable having regard to the interests of data subjects and others, and includes compliance with the requirements of this Law; and

“trade association” includes any body representing data controllers.

(7) The Commissioner shall also provide the Cabinet with a copy of any code of practice prepared under subsection (1), unless the code is included in any report provided to the Cabinet.

(8) The Cabinet shall lay a copy of a report, or of a code provided under subsection (7) before the Legislative Assembly as soon as practicable after the Cabinet receives the report or a copy of the code.

PART 6 - ENFORCEMENT

Complaints

48. (1) A complaint may be made to the Commissioner by or on behalf of any person about any processing of personal data that has not been or is not being carried out in compliance with the provisions of this Law or anything required to be done pursuant to this Law.

(2) On receiving a complaint referred to in subsection (1), or on his own motion, the Commissioner may conduct an investigation.

(3) The matters to which the Commissioner may have regard to in determining whether or not to conduct an investigation referred to in subsection (1) include -

- (a) the extent to which the complaint appears to the Commissioner to raise a matter of substance;
- (b) any undue delay in making the complaint;
- (c) whether any complaint is frivolous or vexatious; and
- (d) whether or not the person making the complaint is entitled to make a request under section 8 in respect of the personal data in question.

49. (1) The Commissioner may require any person to provide him with all such information as he considers appropriate for the purpose of carrying out his functions under this Law including any information with respect to which an exemption is claimed.

Information required by
Commissioner

(2) A person who is required to provide information under this section shall provide it in such a manner, form and within such reasonable period as the Commissioner may specify.

(3) An information requirement under this section shall also contain particulars of the rights of review conferred by section 52.

(4) A person who refuses or, without reasonable excuse, fails to supply information required under subsection (1) commits an offence and is liable to a fine of one hundred thousand dollars or imprisonment for a term of five years, or both.

(5) A person who intentionally alters, suppresses or destroys information that is required to be produced under subsection (1) commits an offence and is liable to a fine of one hundred thousand dollars or imprisonment for a term of five years or both.

(6) A person commits an offence if, in purported compliance with a requirement made under subsection (1), he -

- (a) makes a false statement that the person knows to be false in a material respect; or
- (b) recklessly makes a statement that is false in a material respect,

and is liable to a fine of one hundred thousand dollars or to imprisonment for a term of five years, or to both.

Enforcement orders

50. (1) If the Commissioner is satisfied that there are reasonable grounds for believing that a data controller has contravened, is contravening or is likely to contravene any provisions of this Law, the Commissioner may, by an order served on the data controller, require that data controller to -

- (a) take specified steps within a specified time, or to refrain from taking specified steps after a specified time;
- (b) refrain from processing any personal data, or any personal data of a specified description;
- (c) refrain from processing data for a specified purpose or in a specified manner, after a specified time; or
- (d) do anything which appears to the Commissioner to be incidental or conducive to the carrying out of his functions under this Law.

(2) An enforcement order shall include particulars of the rights of judicial review conferred by section 52.

(3) If -

- (a) an order requires a data controller to rectify, erase or destroy any personal data; or
- (b) the Commissioner is satisfied that personal data that have been rectified, erased or destroyed had been processed in contravention of any of the data protection principles,

that order may, if it is reasonably practicable, require the data controller to notify third parties to whom the data have been disclosed of the rectification, erasure or destruction.

(4) The Commissioner shall, in determining whether it is reasonably practicable to require such an order, have regard in particular to the number of persons who would have to be notified.

Failure to comply with order

51. A person who fails to comply with an information requirement, enforcement order or monetary penalty order under this Law commits an offence and is liable to a fine of one hundred thousand dollars or to imprisonment for a term of five years, or both.

Rights to judicial review

52. A person who has received an information requirement, enforcement order or monetary penalty order under this Law may, within forty-five days of receipt, challenge that requirement or order by seeking judicial review in the Grand Court.

53. (1) Where, upon expiry of the period of forty-five days referred to in section 52 (1) the person concerned has not sought judicial review and has not complied with the information requirement, enforcement order or monetary penalty order, the Commissioner may in writing certify such failure to a summary court. Failure to review

(2) Upon receipt of the certificate referred to in subsection (1) the person concerned shall be deemed to have committed an offence under section 24 of the Summary Jurisdiction Law (2006 Revision) and be dealt with in accordance with that section and any other powers that the summary court may be invested with in relation to contempt committed before it. (2006 Revision)

(3) The Rules Committee referred to in section 39 of the Summary Jurisdiction Law (2008 Revision) may make rules governing -

- (a) the effect, on proceedings referred to in subsection (1), of a person obtaining leave to seek judicial proceedings out of the time referred to in section 52; and
- (b) any other matters relating to proceedings under this section.

54. (1) Except as provided in this Law, no enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing the Commissioner with any information required for the discharge of his functions under this Law. Disclosure of information

(2) Subsection (1) shall not be read so as to compel any individual to utter anything that tends to incriminate him.

55. (1) A current or former Commissioner, current or former member of the Commissioner's staff, current or former agent of the Commissioner, or current or former consultant to the Commissioner, shall not disclose any information which - Confidentiality of information

- (a) has been or was obtained by, or furnished to, the Commissioner under or for the purposes of this Law or the Freedom of Information Law, 2007; (Law 10 of 2007)
- (b) relates to an identified or identifiable person; and
- (c) is not at the time of the disclosure, and has not previously been, available to the public from other sources,

unless the disclosure is made with lawful authority.

(2) For the purposes of subsection (1) a disclosure of information is made with lawful authority only if, and to the extent that -

- (a) the disclosure is made with the consent of the person to whom the information relates;
- (b) the information was provided for the purpose of its being made available to the public, in whatever manner, under any provision of this Law;
- (c) the disclosure is made for the purposes of the discharge of -
 - (i) any functions under this Law or the Freedom of Information Law, 2007; or
 - (ii) any European Union obligation of the United Kingdom that has been extended to the Islands;
- (d) the disclosure is made for the purposes of any proceedings, whether criminal or civil and whether arising under, or by virtue of, this Law or otherwise; or
- (e) having regard to the rights and freedoms or legitimate interests of any person, the disclosure is necessary in the public interest.

(3) A person who knowingly or recklessly discloses information in contravention of subsection (1) commits an offence.

Entry and search of premises, obtaining of information

56. (1) In this Part -

“occupier”, in relation to premises, includes a person in charge of premises;

“premises” includes -

- (a) any ship, aircraft, vessel or other vehicle; and
- (b) any hovercraft or other floating or airborne contrivance.

registered in the Islands.

(2) If a judge is satisfied by information on oath supplied by the Commissioner that there are reasonable grounds for believing -

- (a) that a data controller has contravened, is contravening or is likely to contravene any of the data protection principles; or
- (b) that an offence under this Law has been or is being committed,

and that there are reasonable grounds to believe that evidence of the contravention or of the commission of the offence is to be found on any premises specified in the information, the judge may grant a warrant to the Commissioner.

(3) A warrant issued under subsection (2) may authorize the Commissioner or any of the Commissioner’s staff at any time -

- (a) to enter the premises and search them;

- (b) to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data;
- (c) to inspect, examine and seize any documents, equipment or other thing found there which may be evidence of the contravention of subsection (2).

57. (1) The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of personal data that are exempt under section 24. Warrant not exercisable

(2) The powers of inspection and seizure conferred by a warrant shall not be exercisable in respect of information with respect to which legal professional privilege is claimed; in the event of such a claim, the relevant material shall be sealed, held by a neutral party, and the party claiming privilege shall bring the matter before the Grand Court no later than five working days following such claim, at which time the Grand Court shall determine the matter, and the costs of this procedure shall be in accordance with an order of the Grand Court.

58. A person who -

Offences in respect of warrants

- (a) obstructs a person in the execution of a warrant issued under this Law;
- (b) fails without reasonable excuse to give any person executing such a warrant such assistance as he may reasonably require for the execution of the warrant;
- (c) makes a statement in response to a requirement under this Law which he knows to be false in a material respect; or
- (d) recklessly makes a statement in response to such a requirement which is false in a material respect,

commits an offence and is liable -

- (i) on summary conviction, to a fine of twenty thousand dollars; or
- (ii) on conviction on indictment, to a fine of one hundred thousand dollars or a term of imprisonment of four years, or to both.

59. (1) A person shall not knowingly or recklessly, without the consent of the data controller - Unlawful obtaining etc. of personal data

- (a) obtain or disclose personal data; or
- (b) procure the disclosure to another person of the personal data.

(2) Subsection (1) does not apply to a person who shows -

- (a) that the obtaining, disclosing or procuring -

- (i) was necessary for the purpose of preventing or detecting a crime; or
- (ii) was required or authorized by or under any enactment, by any rule of law or by the order of the Grand Court; or
- (b) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

(3) A person who contravenes subsection (1) commits an offence and is liable, upon conviction, to a fine of one hundred thousand dollars.

(4) A person who sells personal data commits an offence if he has obtained the data in contravention of subsection (1) and is liable, upon conviction, to a fine of one hundred thousand dollars.

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

- (a) he has obtained the data in contravention of subsection (1); or
- (b) he subsequently obtains the data in contravention of that subsection.

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

Power of the
Commissioner to impose
monetary penalty

60. (1) The Commissioner may serve a data controller with a monetary penalty order if the Commissioner is satisfied on a balance of probabilities that -

- (a) there has been a serious contravention of this Law by the data controller; and
- (b) the contravention was of a kind likely to cause substantial damage or substantial distress.

(2) A monetary penalty order is an order requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the order.

(3) The amount of the monetary penalty determined by the Commissioner shall not exceed two hundred and fifty thousand dollars.

(4) The monetary penalty order shall be paid into the general revenues of the Islands within the period specified in the order.

Guidance about
monetary penalty orders

61. (1) The Commissioner shall prepare and issue guidance on the exercise of his functions under section 60.

(2) The guidance shall, in particular, deal with -

- (a) the circumstances in which the Commissioner would consider it appropriate to issue a monetary penalty order, and
- (b) how he will determine the amount of the penalty.

62. (1) A person who commits an offence under this Law is liable, except where this Law otherwise provides - General provisions relating to offences

- (a) on summary conviction, to a fine of ten thousand dollars; or
- (b) on conviction on indictment, to a fine of twenty thousand dollars.

(2) Any fine ordered under this Law shall be in addition to any monetary penalty imposed by the Commissioner under section 60.

(3) The Grand Court by or before which a person is convicted of -

- (a) an offence under section 19, 22 or 59; or
- (b) an offence under section 50 relating to an enforcement order,

may order any document or other material used in connection with the processing of personal data and appearing to the court to be connected with the commission of the offence to be forfeited, destroyed or erased.

(4) The Grand Court shall not make an order under subsection (3) in relation to any material if a person, other than the offender, claiming to be the owner of, or otherwise interested in, the material applies to be heard by the court, unless an opportunity is given to the person to show cause why the order should not be made.

63. (1) Where an offence under this Law has been committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to, any neglect on the part of - Liability for offences

- (a) any director, manager, secretary or similar officer of the body corporate; or
- (b) any person who was purporting to act in any such capacity,

he, as well as the body corporate, commit that offence and are liable to be proceeded against and punished accordingly.

(2) Where the affairs of a 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 the body corporate.

PART 7 - GENERAL

64. (1) This Law binds the Crown. Law binds Crown

65. (1) A notice required by this Law to be given to the Commissioner shall not be regarded as given until it is in fact received by the Commissioner.

(2) A notice or other document required or authorized under this Law or under regulations made under this Law to be given to the Commissioner may be given by electronic or other means by which the Commissioner may obtain or recreate the notice or document in intelligible form.

(3) An order, notice, direction or other document required or authorized by or under this Law to be given to or served on any person other than the Commissioner may be given or served -

- (a) by delivering it to the person;
- (b) by leaving it at the person's address;
- (c) by sending it by post to the person at that address; or
- (d) by sending it to the person at that address by electronic or other means by which the order, notice, direction or document may be obtained or recreated in intelligible form.

(4) Without limiting the generality of subsection (3), any such order, notice, direction or other document may be given to or served on a partnership, company incorporated outside the Islands or unincorporated association by being given to or served -

- (a) in any case, on a person who is, or purports, under whatever description, to act as, its secretary, clerk or other similar officer;
- (b) in the case of a partnership, on the person having the control or management of the partnership business;
- (c) in the case of a partnership or company incorporated outside the Islands, on the local representative referred to in section 6(2); or
- (d) by being delivered to the registered or administrative office of a person referred to in paragraph (a), (b) or (c) if the person is a body corporate.

(5) If the person to or on whom any order, notice, direction or other document referred to in subsection (3) is to be given or served has notified the Commissioner of an address within the Islands as the one at which the person or someone on the person's behalf will accept documents of the same description as that order, notice, direction or other document, that address shall also be treated for the purposes of this section as the person's address.

(6) If the name or the address of an owner, lessee or occupier of premises on whom any order, notice, direction or other document referred to in subsection (3) is to be served cannot after reasonable enquiry be ascertained it may be served by -

- (a) addressing it to the person on whom it is to be served by the description of “owner”, “lessee” or “occupier” of the premises;
- (b) specifying the premises on it; and
- (c) delivering it to a responsible person resident or appearing to be resident on the premises or, if there is no person to whom it can be delivered, by affixing it, or a copy of it, to a conspicuous part of the premises.

66. (1) The Cabinet may make regulations prescribing all matters that are required or permitted by this Law to be prescribed by regulations made by the Cabinet, or are necessary or convenient to be prescribed by regulations made by Cabinet for giving effect to the purposes of this Law. Regulations

- (2) Regulations made under this Law may -
 - (a) make different provisions in relation to different cases or circumstances;
 - (b) apply in respect of particular persons or particular cases or particular classes of persons or particular classes of cases, and define a class by reference to any circumstances whatsoever;
 - (c) contain such transitional, consequential, incidental or supplementary provisions as appear to the Cabinet to be necessary or expedient for the purposes of the regulations; or
 - (d) create an offence punishable by a fine of one hundred thousand dollars.

SCHEDULE 1

(Section 5)

PART 1

THE DATA PROTECTION PRINCIPLES AND THEIR INTERPRETATION

First principle

1. Personal data shall be processed fairly. In addition, personal data may be processed only if -

- (a) in every case, at least one of the conditions set out in paragraphs 1 to 6 of Schedule 2 is met; and
- (b) in the case of sensitive personal data, at least one of the conditions in paragraphs 1 to 10 of Schedule 3 is also met.

Second principle

2. Personal data shall be obtained only for one or more specified lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Third principle

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or processed.

Fourth principle

4. Personal data shall be accurate and, where necessary, kept up to date.

Fifth principle

5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

Sixth principle

6. Personal data shall be processed in accordance with the rights of data subjects under this Law.

Seventh principle

7. Appropriate technical and organisational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Eighth principle

8. Personal data shall not be transferred to a country or territory unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

PART 2

(Section 5(2))

INTERPRETATION OF DATA PROTECTION PRINCIPLES

First principle: source

1. (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to -

- (a) the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed; and
- (b) whether the information contained in the personal data has previously been made public as a result of steps deliberately taken by the data subject.

(2) Subject to paragraph 2, for the purposes of the first principle, personal data are prima facie to be treated as obtained fairly if they consist of information obtained from a person who is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the Islands.

First principle: specified information at relevant time

2. For the purposes of the first principle personal data shall not be treated as processed fairly unless the data subject has, as soon as reasonably practicable, been provided with, at a minimum -

- (a) the identity of the data controller; and
- (b) the purpose for which the data are to be processed.

Seventh principle: processing contract to ensure reliability

3. If processing of personal data is carried out by a data processor on behalf of a data controller, the data controller shall not be regarded as complying with the seventh principle unless the processing is carried out under a contract -

- (a) that is made or evidenced in writing;
- (b) under which the data processor is to act only on instructions from the data controller; and
- (c) that requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

Eighth principle: what is adequate protection in foreign country

4. For the purposes of the eighth principle, an adequate level of protection is one that is adequate in all the circumstances of the case, having regard, among other things, to -

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

Exceptions to eighth principle

5. The eighth principle does not apply to a transfer falling within Schedule 4, except in such circumstances and to such extent as may be prescribed by regulations made by Cabinet.

Eighth principle: European Union finding decisive

6. (1) If in any proceedings under this Law any question arises as to whether the requirement of the eighth principle as to an adequate level of protection is met in relation to the transfer of any personal data to a country or territory outside the Islands which is a member state of the European Union or with respect to which a European Union finding has been made in relation to transfers of the kind in question, that question shall be determined in accordance with that finding.

(2) In this paragraph “European Union finding” means a finding of the European Commission, under the procedure provided for in Article 31(2) of Directive 95/46/EC or such other provision or instrument as may for the time being be in force on the protection of data subjects with regard to the processing of personal data and on the free movement of such data, that a country or territory outside the European Economic Area does, or does not, ensure an adequate level of protection within the meaning of Article 25(2) of the Directive or such other provision or instrument as may for the time being be in force for that purpose.

SCHEDULE 2

(Section 5(3) and Schedule 1, Part 1, paragraph 1(a))

**FIRST PRINCIPLE - CONDITIONS FOR PROCESSING OF ANY
PERSONAL DATA**

Consent

1. The data subject has given consent to the processing.

Processing necessary for contract

2. The processing is necessary for -
 - (a) the performance of a contract to which the data subject is a party;
or
 - (b) the taking of steps at the request of the data subject with a view to entering into a contract.

Processing under legal obligation

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

Processing to protect vital interests

4. The processing is necessary in order to protect the vital interests of the data subject.

Processing necessary for exercise of public functions

5. The processing is necessary for -
 - (a) the administration of justice;
 - (b) the exercise of any functions conferred on any person by or under any enactment;
 - (c) the exercise of any functions of the Crown or any public authority; or
 - (d) the exercise of any other functions of a public nature exercised in the public interest by any person.

Processing for legitimate interests

6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except if the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

Regulations about legitimate interests

7. The Cabinet may, by regulations, specify particular circumstances in which the condition set out in paragraph 6 shall, or shall not, be taken to be satisfied.

SCHEDULE 3

(Section 5(3) and Schedule 1, Part 1, paragraph 1(b))

FIRST PRINCIPLE - CONDITIONS FOR PROCESSING OF SENSITIVE PERSONAL DATA

Consent.

1. The data subject has given consent to the processing of the personal data.

Employment

2. The processing is necessary for the purposes of exercising or performing any right, or obligation, conferred or imposed by law on the data controller in connection with the data subject's employment.

Vital interests

3. The processing is necessary -

- (a) in order to protect the vital interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject; or
- (b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

Non-profit associations

4. The processing -

- (a) is carried out in the course of its legitimate activities by any body, or association, that is not established or conducted for profit, and exists for political, philosophical, religious or trade-union purposes;
- (b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;
- (c) relates only to data subjects who are members of the body or association or have regular contact with it in connection with its purposes; and
- (d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

Information made public by data subject

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

Legal proceedings, etc.

6. The processing -

- (a) is necessary for the purpose of, or in connection with, any legal proceedings;
- (b) is necessary for the purpose of obtaining legal advice; or
- (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Public functions

7. The processing is necessary for -

- (a) the administration of justice;
- (b) the exercise of any functions conferred on any person by or under an enactment; or
- (c) the exercise of any functions of the Crown or any public authority.

Medical purposes

8. (1) The processing is necessary for medical purposes and is undertaken by -

- (a) a health professional; or
- (b) a person who, in the circumstances, owes a duty of confidentiality equivalent to that which would arise if that person were a health professional.

(2) In this paragraph, “medical purposes” includes the purposes of preventative medicine, medical diagnosis, the provision of care and treatment, and the management of healthcare services.

Circumstances prescribed by regulations

9. The personal data are processed in such circumstances as may be prescribed by regulations made by Cabinet.

Regulations relating to paragraph 2 or 7

10. The Cabinet may by regulations -

- (a) exclude the application of paragraph 2 or 7 in such cases as may be specified; or
- (b) provide that, in such cases as may be specified, the condition in paragraph 2 or 7 shall not be regarded as satisfied unless such further conditions as may be specified in the regulations are also satisfied.

SCHEDULE 4

(Section 5(3) and Schedule 1, Part 2, paragraph 14)

TRANSFERS TO WHICH EIGHTH PRINCIPLE DOES NOT APPLY

Consent

1. The data subject has consented to the transfer.

Contract between data subject and data controller

2. The transfer is necessary for -

- (a) the performance of a contract between the data subject and the data controller; or
- (b) the taking of steps at the request of the data subject with a view to the data subject's entering into a contract with the data controller.

Third-party contract in interest of data subject

3. The transfer is necessary for -
- (a) the conclusion of a contract between the data controller and a person other than the data subject, being a contract that is entered into at the request of the data subject, or is in the interests of the data subject; or
 - (b) the performance of such a contract.

Public interest

4. The transfer is necessary for reasons of substantial public interest.

Legal proceedings, etc.

5. The transfer -
- (a) is necessary for the purpose of, or in connection with, any legal proceedings;
 - (b) is necessary for the purpose of obtaining legal advice; or
 - (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Vital interests

6. The transfer is necessary in order to protect the vital interests of the data subject.

Public register

7. The transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.

Transfer made on terms approved by Commissioner

8. The transfer is made on terms of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects.

Commissioner has authorized transfer

9. The transfer has been authorized by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

International cooperation between intelligence agencies

10. The transfer is required under international cooperation arrangements between intelligence agencies to combat organized crime, terrorism or drug trafficking.

Regulations concerning the public interest

11. The Cabinet may, by regulations, specify in broad, non-exhaustive terms -

- (a) circumstances in which a transfer shall be taken for the purposes paragraph 4 to be necessary for reasons of substantial public interest; and
- (b) circumstances in which a transfer not required by or under an enactment shall not be taken, for the purposes of paragraph 4, to be necessary for reasons of substantial public interest.

SCHEDULE 5

(Section 2(1))

CONDITIONS OF CONSENT

1. The data controller shall bear the burden of proving the data subject's consent to the processing of their personal data for the specified purposes.

2. If the data subject's consent is to be given in the form of a written declaration which also concerns another matter, the requirement to give consent shall be presented in an appearance that is distinguishable from the other matter.

3. The data subject shall have the right to withdraw his consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

4. Where there is a significant imbalance between the position of the data subject and the data controller, consent shall not provide a legal basis for the processing.

Passed by the Legislative Assembly the day of , 2014.

Speaker.

Clerk of the Legislative Assembly.