

Session: 2002
Bill No. 26

Hon. Perry G. Christie
or a member of government
23 January, 2003

A BILL

for

AN ACT TO PROTECT THE PRIVACY OF INDIVIDUALS
IN RELATION TO PERSONAL DATA AND TO REGULATE
THE COLLECTION, PROCESSING, KEEPING, USE AND
DISCLOSURE OF CERTAIN INFORMATION RELATING
TO INDIVIDUALS AND TO PROVIDE FOR MATTERS
INCIDENTAL THERETO OR CONNECTED THEREWITH.

Enacted by the Parliament of The Bahamas

PART I
PRELIMINARY

Short title
and com-
mencement.

1. (1) This Act may be cited as the Data
Protection(Privacy of Personal Information) Act, 2003.

(2) This Act shall come into operation on such
day as the Minister may, by notice published in the Gazette,
appoint.

Interpre-
tation.

2. (1) In this Act -

"back-up data" means data kept only for the purpose of
replacing other data in the event of their being
altered, lost, destroyed or damaged;

"the Commissioner" means the Data Protection
Commissioner established under section 14;

"company" has the meaning assigned to it by the

Companies Act, 1992 or an International Business Company under the International Business Companies Act, 2000;

"the Court" means the Supreme Court or a judge thereof;

"data" means information in a form in which it can be processed;

"data controller" means a person who, either alone or with others, determines the purposes for which and the manner in which any personal data are, or are to be, processed;

"data equipment" means equipment for processing data;

"data material" means any document or other material used in connection with, or produced by, data equipment;

"data processor" means a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment;

"data subject" means an individual who is the subject of personal data;

"days" means working days;

"direct marketing" includes direct mailing;

"disclosure", in relation to personal data, includes the disclosure of information extracted from such data but does not include a disclosure made directly or indirectly by a data controller to an employee or agent of his or to a data processor for the purpose of enabling the employee, agent or data processor to carry out his duties; and, where the identification of a data subject depends partly on the data and partly on other information in the possession of the data controller, the data shall

not be regarded as disclosed unless the other information is also disclosed;

First
Schedule.

"enforcement notice" means a notice issued by the Commissioner under section 16;

"government agency" means any Ministry or department of Government, or any body or office specified in the First Schedule, which Schedule may be amended by the Minister by Order from time to time;

First
Schedule.

"head" means in respect of a government agency, the designated officer appearing in the second column corresponding with the government agency in the first column, of the First Schedule;

"information notice" means a notice issued by the Commissioner under section 18;

"the Minister" means the Minister with responsibility for Information Privacy and Data Protection;

"personal data" means data relating to a living individual who can be identified either from the data or from the data in conjunction with other information in the possession of the data controller;

"processing" , in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including -

- (a) organisation, adaptation or alteration of the information or data;
- (b) retrieval, consultation or use of the information or data;
- (c) transmission of data;
- (d) dissemination or otherwise making available; or
- (e) alignment, combination, blocking, erasure

or destruction of the information or data;

"prohibition notice" means a notice served under section 17;

Ch. 31.

"public officer" has the meaning assigned to it by the Public Service Act;

"sensitive personal data" means personal data relating to -

- (a) racial origin;
- (b) political opinions or religious or other beliefs;
- (c) physical or mental health (other than any such data reasonably kept by them in relation to the physical or mental health of their employees in the ordinary course of personnel administration and not used or disclosed for any other purpose);
- (d) trade union involvement or activities;
- (e) sexual life; or
- (f) criminal convictions, the commission or alleged commission of any offence, or any proceedings for any offence committed, the disposal of such proceedings or the sentence of any court in such proceedings.

(2) For the purposes of this Act, data are inaccurate if they are incorrect or misleading as to any matter of fact:

Provided that this section shall not have been contravened by a data controller as respects any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in any case where -

- (a) having regard to the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data; and
- (b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact.

Crown to
be bound.

3. (1) This Act binds the Crown.

(2) Where a government agency, satisfies the conditions for being a data controller or a data processor under this Act, the head of such institution shall be deemed, for the purposes of this Act, to be a data controller or, as the case may be, a data processor.

(3) For the purposes of this Act, as respects any personal data, all other public officers or employees, as the case may be, within the same institution, shall be deemed to be employees of the designated head in the case of a designation provided for in subsection (2).

Application
of Act.

4. (1) Except as otherwise provided for herein, this Act applies to a data controller in respect of any data only if -

- (a) the data controller is established in The Bahamas and the data are processed in the context of that establishment; or
- (b) the data controller is not established in The Bahamas but uses equipment in The Bahamas for processing the data otherwise than for the purpose of transit through The Bahamas.

(2) A data controller falling within subsection (1)(b) must nominate for the purposes of this Act a

representative established in The Bahamas.

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

- (a) an individual who is ordinarily resident in The Bahamas;
- (b) a body incorporated or registered under the laws of The Bahamas;
- (c) a partnership or other unincorporated association formed under the laws of The Bahamas; and
- (d) any person who does not fall within paragraph (a), (b) or (c) but, maintains in The Bahamas an office, branch or agency through which he carries on any business activity or a regular practice.

Exclusions
to Act.

5.

This Act shall not apply to personal data -

- (a) that in the opinion of the Minister or the Minister for National Security are, or at any time were, kept for the purpose of safeguarding the security of The Bahamas;
- (b) consisting of information that the person keeping the data is required by law to make available to the public;
- (c) kept by an individual and concerned only with the management of his personal, family or household affairs or kept by an individual only for recreational purposes;
- (d) deliberations of Parliament and Parliamentary committees; or
- (e) pending civil, criminal or international

legal assistance procedures.

PART II
PROTECTION OF PRIVACY OF INDIVIDUALS
WITH REGARD TO PERSONAL DATA

Collection,
processing,
keeping,
use and
disclosure
of personal
data.

6. (1) A data controller shall comply with the following provisions in relation to personal data kept by him -

- (a) the data or the information constituting the data shall have been collected by means which are both lawful and fair in the circumstances of the case;
- (b) the data is accurate and, where necessary, kept up to date, (except in the case of back-up data);
- (c) the data -
 - (i) shall be kept only for one or more specified and lawful purposes,
 - (ii) shall not be used or disclosed in any manner incompatible with that purpose or those purposes,
 - (iii) shall be adequate, relevant and not excessive in relation to that purpose or those purposes, and
 - (iv) shall not be kept for longer than is necessary for that purpose or those purposes, except in the case of personal

data kept for historical, statistical or research purposes; and

- (d) appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.

(2) In determining for the purposes of subsection (1)(a) of this section, whether personal data or information constituting such data are fair in the circumstances of the case, regard is to be had to 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:

Provided however that the data or the information constituting such data shall not be regarded for the purposes of subsection (1)(a) of this section as having been obtained unfairly by reason only that its use for any such purpose was not disclosed when it was obtained, if the data are not used in such a way that damage or distress is, or is likely to be, caused to any data subject.

(3) A data processor shall, as respects personal data processed by him, comply with subsection (1)(d) of this section.

Exceptions
to section
6.

7. Subsection (1)(a) of section 6 shall not apply to information intended for inclusion in data, or to data, kept for a purpose mentioned in paragraph (a) of section 9, in any case in which the application of that paragraph to the data would be likely to prejudice any of the matters mentioned in paragraph (a) of section 9.

Right of
access.

8. (1) Subject to the provisions of this Act, any individual who makes a written request to a data controller

has a right, within forty days after complying with the provisions of this section, to -

- (a) be informed by the data controller whether the data kept by him include personal data relating to the individual;
- (b) be supplied by the data controller with a copy of the information constituting any such data; and
- (c) where any of the information is expressed in terms that are not intelligible to the average person without explanation, the information shall be accompanied by an explanation of those terms.

(2) A request for the information specified in subsection (1)(a) shall, in the absence of any indication to the contrary, be treated as including a request for a copy of the information specified in subsection (1)(b).

(3) The Minister may by regulations prescribe the fee to be charged by a data controller in respect of such a request as aforesaid, and any fee so paid shall be reimbursed where the request is not complied with or the data controller rectifies, supplements, or erases part of, the data concerned (and thereby materially modifies the data) or erases all of the data on the application of the individual or in accordance with an enforcement notice hereunder or court order.

(4) An individual making a request under this section shall supply the data controller concerned with such information as he may reasonably require in order to satisfy himself of the identity of the individual and to locate any relevant personal data or information.

(5) Nothing in subsection (1) obliges a data controller to disclose to a data subject personal data relating to another individual unless that other individual

has consented to the disclosure:

Provided that, where the circumstances are such that it would be reasonable for the data controller to conclude that, if any particulars identifying that other individual were omitted, the data could then be disclosed as aforesaid without his being thereby identified to the data subject, the data controller shall be obliged to disclose the data to the data subject with the omission of those particulars.

(6) Information supplied pursuant to a request under subsection (1) may take account of any amendment of the personal data concerned made since the receipt of the request by the data controller (being an amendment that would have been made irrespective of the receipt of the request) but not of any other amendment.

(7) A notification of a refusal of a request made by an individual under the preceding provisions of this section shall be in writing and shall include a statement of the reasons for the refusal and an indication that the individual may complain to the Commissioner about the refusal.

(8) Where a data controller has previously complied with a request made under subsection (1) by an individual, the data controller is not obliged to comply with a subsequent, identical or similar request under that subsection by that individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request.

(9) In determining for the purposes of subsection (8) whether requests under subsection (1) are made at reasonable intervals, regard shall be had to the nature of the data, the purposes for which the data are processed and the frequency with which the data are altered.

Exceptions

9. Section 8 shall not apply to personal data -

to right
of access.

- (a) kept for the purpose of preventing, detecting or investigating an offence or a breach of agreement, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the Government, a local authority, a statutory corporation, or a public body, in any case in which the application of that section to the data would be likely to prejudice any of the matters aforesaid;
- (b) to which, by virtue of paragraph (a) section 8 does not apply and which are kept for the purpose of discharging a function conferred by or under any enactment and consisting of information obtained for such a purpose from a person who had it in his possession for any of the purposes mentioned in paragraph (a);
- (c) in any case in which the application of section 8 would be likely to prejudice the security of, or the maintenance of good order and discipline in a prison, a place of detention provided under the Prisons Act, or any other enactment under the laws of The Bahamas;
- (d) kept for the purpose of performing such functions conferred by or under any enactment as may be specified by regulations made by the Minister, being functions that, in the opinion of the Minister, are designed to protect members of the public against financial

Ch. 193.

loss in any case in which the application of that section to the data would be likely to prejudice the proper performance of any of those functions, occasioned by –

- (i) dishonesty, incompetence or malpractice on the part of persons concerned in the provision of banking, insurance, investment or other financial services or in the management of companies or similar organisations, or
 - (ii) the conduct of persons who have at any time been adjudicated bankrupt;
- (e) in respect of which the application of that section would be contrary to the interests of protecting the international relations of The Bahamas;
- (f) consisting of an estimate of, or kept for the purpose of estimating, the amount of the liability of the data controller concerned based on a claim for the payment of a sum of money, whether in respect of damages or compensation, in any case in which the application of section 8 would be likely to prejudice the interests of the data controller in relation to the claim;
- (g) in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications

between a client and his professional legal advisers or between those advisers;

- (h) kept only for the purpose of preparing statistics or carrying out research if the data are not used or disclosed (other than to a person to whom a disclosure of such data may be made in the circumstances specified in section 13) for any other purpose and the resulting statistics or the results of the research are not made available in a form that identifies any of the data subjects;
- (i) in any case in which the application of that section would reveal confidential commercial information which cannot be severed from the record containing the personal information for which access is requested; or
- (j) that are back-up data.

Right of
rectifi-
cation or
erasure.

10. (1) An individual shall, upon submission of a written request to a data controller who keeps personal data relating to him, be entitled to have rectified or, where appropriate, erased any such data in relation to which there has been a contravention of subsection (1) of section 6 by the data controller and the data controller shall comply with the request within forty days after it has been given or sent to him:

Provided that the data controller shall, as respects data that are inaccurate or not kept up to date, be deemed -

- (a) to have complied with the request if he supplements the data with a statement (to the terms of which the individual has

agreed) relating to the matters dealt with by the data; and

- (b) if he supplements the data as aforesaid, not to be in contravention of subsection (1)(b) of section 6.

(2) In complying with a request under subsection (1) of this section, a data controller shall, within forty days after the request has been given or sent to him, notify the individual making the request of such compliance.

Right to prohibit processing for purposes of direct marketing.

11. Where a data subject makes a written request for the data controller to cease using, for the purpose of direct marketing, any data which was kept for that purpose, the data controller shall, as soon as may be and in any event not more than forty days after the request has been given or sent to him -

- (i) erase all data as was kept for the purpose aforesaid, or
- (ii) if the data are kept for that purpose and other purposes, cease using the data for that purpose, and
- (iii) notify the data subject in writing accordingly.

Duty of care owed by data controllers.

12. (1) A person, being a data controller shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned:

Provided that, for the purposes of this section, a data controller shall be deemed to have complied with the provisions of subsection (1)(b) of section 6 if and so long as the personal data concerned accurately record data or other information received or obtained by him from the data

subject or a third party and include (and, if the data are disclosed, the disclosure is accompanied by) -

- (a) an indication that the information constituting the data was received or obtained as aforesaid;
- (b) if appropriate, an indication that the data subject has informed the data controller that he regards the information as inaccurate or not kept up to date; and
- (c) any statement with which, pursuant to this Act, the data are supplemented.

(2) A data controller shall use contractual or other legal means to provide a comparable level of protection from any third party to whom he discloses information for the purpose of data processing.

Disclosure
of personal
data in
certain
cases.

13. In this Act any restrictions on or exceptions to the disclosure of personal data do not apply if the disclosure is -

- (a) in the opinion of the Minister or the Minister of National Security required for the purpose of safeguarding the security of The Bahamas;
- (b) required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the Government, statutory corporation, public body, or a local authority, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid;

- (c) required in the interests of protecting the international relations of The Bahamas;
- (d) required urgently to prevent injury or other damage to the health of a person or serious loss of or damage to property;
- (e) required by or under any enactment or by a rule of law or order of a court;
- (f) required for the purposes of obtaining legal advice or for the purposes of, or in the course of, legal proceedings in which the person making the disclosure is a party or a witness;
- (g) made to the data subject concerned or to a person acting on his behalf; or
- (h) made at the request or with the consent of the data subject or a person acting on his behalf.

PART III

THE DATA PROTECTION COMMISSIONER

The Com-
missioner.

14. (1) For the purposes of this Act, there shall be a person who shall be known as the Data Protection Commissioner and who shall perform the functions conferred on him by this Act.

Second
Schedule.

(2) The Commissioner shall be a corporation sole.

(3) The provisions of the Second Schedule shall have effect in relation to the Commissioner.

Enforcement

15. (1) The Commissioner may investigate, or cause to

of data protection.

be investigated, whether any of the provisions of this Act have been, are being or are likely to be contravened by a data controller or a data processor in relation to an individual either where the individual complains to him of a contravention of any of those provisions or he is otherwise of the opinion that there may be such a contravention.

(2) Where a complaint is made to the Commissioner under subsection (1), the Commissioner shall -

(a) investigate the complaint or cause it to be investigated, unless he is of the opinion that it is frivolous or vexatious; and

(b) as soon as may be, notify the individual concerned in writing of his decision in relation to the complaint and that the individual may, if aggrieved by his decision, appeal against the decision under section 24.

(3) If the Commissioner is of the opinion that a data controller or a data processor, has contravened or is contravening a provision of this Act (other than a provision the contravention of which is an offence), the Commissioner may, by notice in writing (referred to in this Act as an enforcement notice) served on the person, require him to take such steps as are specified in the notice within such time as may be so specified to comply with the provision concerned.

(4) Without prejudice to the generality of subsection (3), if the Commissioner is of the opinion that a data controller has contravened section 6, the relevant enforcement notice may require him -

(a) to rectify or erase any of the data concerned; or

(b) to supplement the data with such

statement relating to the matters dealt with by them as the Commissioner may approve; and as respects data that are inaccurate or not kept up to date, if he supplements them as aforesaid, he shall be deemed not to be in contravention of subsection (1)(b) of section 6.

Enforcement notices.

16. (1) The Commissioner may issue an enforcement notice which shall -

- (a) specify any provision of this Act that, in the opinion of the Commissioner, has been or is being contravened and the reasons for his having formed that opinion; and
- (b) subject to subsection (2), state that the person concerned may appeal to the Court under section 24 against the requirement specified in the notice within twenty-one days from the service of the notice on him.

(2) Subject to subsection (3), the time specified in an enforcement notice for compliance with a requirement specified therein shall not be expressed to expire before the end of the period of twenty-one days specified in subsection (1) (b) and, if an appeal is brought against the requirement, the requirement need not be complied with and subsection (6) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(3) If the Commissioner -

- (a) by reason of special circumstances, is of the opinion that a requirement specified in an enforcement notice should be complied with urgently; and

(b) such enforcement notice includes a statement to that effect, subsections (1)(b) and (2) shall not apply in relation to the notice, but the notice shall contain a statement of the effect of the provisions of section 24 (other than subsection (2)) and shall not require compliance with the requirement before the end of the period of seven days beginning on the date on which the notice is served.

(4) On compliance by a data controller with a requirement under subsection (4) of section 15, he shall, as soon as may be and in any event not more than forty days after such compliance, notify -

- (a) the data subject concerned; and
- (b) any person (where the Commissioner considers it reasonably practicable to do so) to whom the data were disclosed during the period beginning twelve months before the date of the service of the enforcement notice concerned and ending immediately before such compliance, of the rectification, erasure or statement concerned, if such compliance materially modifies the data concerned.

(5) The Commissioner may cancel an enforcement notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(6) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an enforcement notice shall be guilty of an offence.

Prohibition
on transfer
of personal
data out-

17. (1) The Commissioner may, subject to the provisions of this section, prohibit the transfer of personal data from The Bahamas to a place outside The Bahamas, in such cases where there is a failure to provide protection either by

side The
Bahamas.

contract or otherwise equivalent to that provided under this Act.

(2) In determining whether to prohibit a transfer of personal data under this section, the Commissioner shall also consider whether the transfer would be likely to cause damage or distress to any person and have regard to the desirability of facilitating international transfers of data.

(3) A prohibition under subsection (1) shall be effected by the service of a notice (referred to in this Act as a prohibition notice) on the person proposing to transfer the data concerned.

(4) A prohibition notice shall -

- (a) prohibit the transfer concerned either absolutely or until the person aforesaid has taken such steps as are specified in the notice for protecting the interests of the data subjects concerned;
- (b) specify the time when it is to take effect;
- (c) specify the grounds for the prohibition; and
- (d) subject to subsection (6), state that the person concerned may appeal to the Court under section 24 against the prohibition specified in the notice within twenty-one days from the service of the notice on him.

(5) Subject to subsection (6), the time specified in a prohibition notice for compliance with the prohibition specified therein shall not be expressed to expire before the end of the period of the twenty-one days specified in subsection (4) (d) and, if an appeal is brought against the prohibition, the prohibition need not be complied with and

subsection (10) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(6) If the Commissioner -

(a) by reason of special circumstances, is of the opinion that a prohibition specified in a prohibition notice should be complied with urgently; and

(b) such prohibition notice includes a statement to that effect,

subsections(4)(d) and(5) shall not apply in relation to the notice but the notice shall contain a statement of the effect of the provisions of section 24 (other than subsection (2)) and shall not require compliance with the prohibition before the end of the period of seven days beginning on the date on which the notice is served.

(7) The Commissioner may cancel a prohibition notice and, if he does so, shall notify in writing the person on whom it was served accordingly.

(8) This section shall not apply to a transfer of data if the transfer of the data or the information constituting the data is required or authorised by or under any enactment, or required by any convention or other instrument imposing an international obligation on The Bahamas, or otherwise made pursuant to the consent (express or implied) of the data subjects.

(9) This section applies, with any necessary modifications, to a transfer of information from The Bahamas to a place outside The Bahamas for conversion into personal data as it applies to a transfer of personal data from The Bahamas to such a place; and in this subsection "information" means information (not being data) relating to a living individual who can be identified from it.

(10) A person who, without reasonable excuse, fails

or refuses to comply with a prohibition specified in a prohibition notice shall be guilty of an offence.

Power to
require
information.

18. (1) The Commissioner may, by notice in writing (referred to in this Act as an information notice) served on a person, require the person to furnish to him in writing within such time as may be specified in the notice such information in relation to matters specified in the notice as is necessary or expedient for the performance by the Commissioner of his functions.

(2) Subject to subsection (3) -

(a) an information notice shall state that the person concerned may appeal to the Court under section 24 against the requirement specified in the notice within twenty-one days from the service of the notice on him; and

(b) the time specified in the notice for compliance with a requirement specified therein shall not be expressed to expire before the end of the period of twenty-one days specified in paragraph (a) and, if an appeal is brought against the requirement, the requirement need not be complied with and subsection (5) shall not apply in relation thereto, pending the determination or withdrawal of the appeal.

(3) If the Commissioner -

(a) by reason of special circumstances, is of the opinion that a requirement specified in an information notice should be complied with urgently; and

(b) such information notice includes a

statement to that effect, subsection (2) shall not apply in relation to the notice, but the notice shall contain a statement of the effect of the provisions of section 24 (other than subsection (2)) and shall not require compliance with the requirement before the end of the period of seven days beginning on the date on which the notice is served.

(4) No enactment or rule of law prohibiting or restricting the disclosure of information shall preclude a person from furnishing to the Commissioner any information that is necessary or expedient for the performance by the Commissioner of his functions and this subsection shall not apply to information that in the opinion of the Minister or the Minister for National Security is, or at any time was, kept for the purpose of safeguarding the security of The Bahamas or information that is privileged from disclosure in proceedings in any court.

(5) A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an information notice or who in purported compliance with such a requirement furnishes information to the Commissioner that the person knows to be false or misleading in a material respect shall be guilty of an offence.

Powers of
authorised
officer.

19. (1) In this section "authorised officer" means a person authorised in writing by the Commissioner to exercise the powers conferred by this section, for the purposes of this Act.

(2) Where a Magistrate is satisfied by evidence on oath that there is reasonable cause to believe that for the purpose of obtaining any information that is necessary or expedient for the performance by the Commissioner of his functions, he may grant a warrant directed to an authorised officer to -

- (a) enter, at all reasonable times, premises that he reasonably believes to be occupied by a data controller or a data processor, inspect the premises and any data therein (other than data consisting of information specified in subsection (4) of section 18) and inspect, examine, operate and test any data equipment therein;
- (b) require any person on the premises, being a data controller, a data processor or an employee of either of them, to disclose to the officer any such data and produce to him any data material (other than data material consisting of information so specified) that is in that person's power or control and to give to him such information as he may reasonably require in regard to such data and material;
- (c) either on the premises or elsewhere, inspect and copy or extract information from such data, or inspect and copy or take extracts from such material; and
- (d) require any person mentioned in paragraph (b) to give to the officer such information as he may reasonably require in regard to the procedures employed for complying with the provisions of this Act, the sources from which such data are obtained, the purposes for which they are kept, the persons to whom they are disclosed and the data equipment in the premises.

(3) A person who obstructs or impedes an authorised officer in the exercise of a power, or without reasonable excuse does not comply with a requirement under this section, or who in purported compliance with such a requirement gives information to an authorised officer that he knows to be false or misleading in a material respect shall be guilty of an offence.

Codes of
practice.

20. (1) The Commissioner may encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in dealing with personal data.

(2) The Commissioner may approve of any code of practice so prepared (referred to subsequently in this section as a code) if he is of opinion that it provides for the data subjects concerned protection with regard to personal data relating to them that conforms with that provided for by sections 6, 8 (other than subsection (9)) and 10 and shall encourage its dissemination to the data controllers concerned.

(3) Any such code that is approved by the Commissioner shall be laid by the Minister before each House of Parliament and shall be subject to affirmative resolution of each House.

(4) In subsection (3), "affirmative resolution of each House" means that such code shall not come into operation unless and until affirmed by a resolution of each House of Parliament.

(5) This section shall apply in relation to data processors as it applies in relation to categories of data controllers with the modification that the references in this section to the said sections shall be construed as references to subsection (1)(d) of section 6 and with any other necessary modifications.

Annual

21. (1) The Commissioner shall in each year after the

report.

year in which the first Commissioner is appointed prepare a report in relation to his activities under this Act in the preceding year and cause copies of the report to be laid before each House of Parliament.

(2) Notwithstanding subsection (1), if, but for this subsection, the first report under that subsection would relate to a period of less than six months, the report shall relate to that period and to the year immediately following that period and shall be prepared as soon as may be after the end of that year.

PART IV

MISCELLANEOUS

Unauthorised disclosure by data processor.

22. (1) Personal data processed by a data processor shall not be disclosed by him, or by an employee or agent of his, without the prior authority of the data controller on behalf of whom the data are processed.

(2) A person who knowingly contravenes subsection (1) shall be guilty of an offence.

Disclosure of personal data obtained without authority.

23. (1) A person who -

(a) obtains access to personal data, or obtains any information constituting such data, without the prior authority of the data controller or data processor by whom the data are kept; and

(b) discloses the data or information to another person, shall be guilty of an offence.

(2) Subsection (1) shall not apply to a person who is an employee or agent of the data controller or data

processor concerned.

Appeals to
Court.

24. (1) An appeal may be made to and heard and determined by the Court against –

- (a) a requirement specified in an enforcement notice or an information notice;
- (b) a prohibition specified in a prohibition notice; or
- (c) a decision of the Commissioner in relation to a complaint under subsection (1) of section 15;

and such an appeal shall be brought within twenty-one days from the service on the person concerned of the relevant notice or, as the case may be, the receipt by such person of the notification of the relevant refusal or decision.

(2) Where –

- (a) a person appeals to the Court pursuant to paragraph (a), (b) or (c) of subsection (1);
- (b) the appeal is brought within the period specified in the notice; and
- (c) the Commissioner has included a statement in the relevant notice or notification to the effect that by reason of special circumstances he is of opinion that the requirement or prohibition specified in the notice should be complied with, or the refusal specified in the notification should take effect, urgently,

then, notwithstanding any provision of this Act, if the Court, on application made to it in that behalf, so determines, non-compliance by the person with a requirement or prohibition specified in the notice during the period ending with the determination or withdrawal of the appeal or during such other

period as may be determined as aforesaid shall not constitute an offence.

Evidence
in pro-
ceedings.

25. (1) In any proceedings –

(a) a certificate signed by the Minister or the Minister for National Security and stating that in his opinion personal data are, or at any time were, kept for the purpose of safeguarding the security of The Bahamas shall be evidence of that opinion; or

(b) a certificate –

(i) signed by an officer on behalf of the Minister or Minister of National Security, and

(ii) stating that in the opinion of the officer a disclosure of personal data is required for the purpose aforesaid,

shall be evidence of that opinion; and

(c) a document purporting to be a certificate under paragraph (a) or (b) of, and signed by, a person specified in the said paragraph (a) or (b) shall be deemed to be such a certificate and to be so signed unless the contrary is proved.

(2) Information supplied by a person in compliance with a request made under section 6 or subsection (1) of section 8, a requirement under this Act or a direction of a court in proceedings under this Act shall not be admissible in evidence against him or his spouse in proceedings for an offence under this Act.

Hearing
of pro-

26. The whole or any part of any proceedings under this Act may, at the discretion of the Court, be heard

ceedings.

otherwise than in public.

Offences by directors, etc. of bodies corporate.

27. (1) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of a person, being a director, manager, secretary or other officer of that body corporate, or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and be liable to be proceeded against and punished accordingly.

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

Prosecution of summary offences by Commissioner.

28. (1) Summary proceedings for an offence under this Act may be brought and prosecuted by the Commissioner.

(2) Notwithstanding any provision in any enactment prescribing the period within which summary proceedings may be commenced, summary proceedings for an offence under this Act may be instituted within one year from the date of the offence.

Penalties.

29. (1) A person guilty of an offence under this Act shall be liable –

(a) on summary conviction, to a fine not exceeding two thousand dollars; or

(b) on conviction on information, to a fine not exceeding one hundred thousand dollars.

(2) Where a person is convicted of an offence under this Act, the court may order any data material which appears to the court to be connected with the commission of the offence to be forfeited or destroyed and any relevant data

to be erased.

(3) The court shall not make an order under subsection (2) in relation to data material or data where it considers that some person other than the person convicted of the offence concerned may be the owner of, or otherwise interested in, the data unless such steps as are reasonably practicable have been taken for notifying that person and giving him an opportunity to show cause why the order should not be made.

Regulations.

30. (1) The Minister may, from time to time make regulations for all or any of the following purposes -

- (a) providing additional safeguards in relation to sensitive personal data;
- (b) modifying the application of section 8 to personal data in such manner and in such circumstances, subject to such safeguards and to such extent as may be specified therein, where such data -
 - (i) relates to physical or mental health, or
 - (ii) is kept for, or obtained in the course of, carrying out social work by a government agency, a statutory corporation, or a specified voluntary organisation or other body;
- (c) prescribing circumstances for the purposes of section 9 in which a prohibition, restriction or authorisation in relation to any information ought to prevail in the interests of the data subjects concerned or any other individuals;

- (d) prescribing fees to be paid in respect of matters arising under or provided for or authorised by this Act;
- (e) prescribing offences and penalties in respect of contravention of or non-compliance with any provision of any regulations made under this section;
- (f) providing for such matters as are contemplated by or necessary for giving full effect to the provisions of this Act and for their due administration.

(2) Regulations made under paragraph (a) of subsection (1) are subject to affirmative resolution of each House of Parliament and shall be made only after consultation with any other Minister of the Government who, having regard to his functions, ought, in the opinion of the Minister, to be consulted.

(3) In subsection (2), "affirmative resolution of each House" means that such regulations shall not come into operation unless and until affirmed by a resolution of each House of Parliament.

Transi-
tional
provisions.

31. (1) Within one year after the coming into force of this Act data controllers shall have the necessary measures in place that would allow the exercise of a request for access, pursuant to section 8.

(2) Notwithstanding any other provision contained herein to the contrary, Government agencies and other bodies specified in the First Schedule may continue for a period of five years from the date of entry into force of this Act, to use and process existing files that contain personal data including sensitive personal data which were acquired in circumstances in which it is not possible to determine if such was obtained in pursuance of a legal obligation or with the

consent of the data subjects.

FIRST SCHEDULE

(Section 2)

1. The Government.
2. A Government Ministry.
3. A local government authority, and any other body (other than the Royal Bahamas Police and Defence Forces) established –
 - (a) by or under any enactment (other than the Companies Acts, 1992), or
 - (b) under the Companies Acts, 1992 in pursuance of powers conferred by or under another enactment, and financed wholly or partly by means of moneys provided, or loans made or guaranteed, by the Government or the issue of shares held by or on behalf of the Government; and a subsidiary of any such body.
4. A company the majority of the shares in which are held by or on behalf of the Government.
5. A body (other than a body mentioned in paragraph 3 or 4) appointed by the Government or a Minister of the Government.
6. An individual (other than an individual remunerated by a body mentioned in paragraph 3, 4 or 5 or in

relation to whom the Government or a Minister of the Government is the appropriate authority) who is appointed by the Government or a Minister of the Government to an office established by or under any enactment.

7. Any other public authority, body or person prescribed for the time being and financed or remunerated wholly or partly out of moneys provided from the consolidated fund.

Government Ministries/
Departments etc.

Ministries
Departments

Designated Heads

Accounting Officer
Heads of Departments

SECOND SCHEDULE

(Section 14)

THE DATA PROTECTION COMMISSIONER

1. The Commissioner shall be a corporation sole and shall be independent in the performance of his functions.

2. (1) The Commissioner shall be appointed in writing by the Governor-General acting on the advice of the Prime Minister after consultation with the Leader of the Opposition.

(2) The Commissioner –

(a) may at any time resign his office as Commissioner by letter addressed to the Governor-General and the resignation shall take effect on and from the date of receipt of the letter;

(b) may at any time be removed from

office by the Governor-General on the advice of the Prime Minister after consultation with the Leader of the Opposition if, in the opinion of the Prime Minister, he has become incapable of effectively performing his functions or has committed a misbehaviour; and

- (c) shall, in any case, vacate the office of Commissioner on reaching the age of sixty-five years.

3. The term of office of a person appointed to be the Commissioner shall be such term not exceeding five years and, subject to the provisions of this Schedule, he shall be eligible for re-appointment to the office.

4. (1) Where the Commissioner is -

- (a) nominated as a member of the Senate;
(b) elected as a member of the House of Assembly or a local authority,

he shall thereupon cease to be the Commissioner.

(2) A person who is for the time being -

- (a) a member of either House of Parliament;
(b) an elected local government member, shall, while he is so entitled or is such a member, be disqualified from holding the office of Commissioner.

5. The Commissioner shall not hold any other office or employment in respect of which emoluments are payable.

6. There shall be paid to the Commissioner, out of moneys provided from the Consolidated Fund, such remuneration and allowances for expenses as the Minister, with the consent of the Minister for Finance, may from time to time determine.

7. The Minister -

(a) shall, with the consent of the Minister for Finance, make and carry out, in accordance with its terms, a scheme or schemes for the granting of pensions, gratuities or other allowances on retirement or death to or in respect of persons who have held the office of Commissioner;

(b) may, with the consent of the Minister for Finance, at any time make and carry out, in accordance with its terms, a scheme or schemes amending or revoking a scheme under this paragraph,

and a scheme under this paragraph shall be laid before each House of Parliament as soon as may be after it is made and, if a resolution annulling the scheme is passed by either such House within the next twenty-one days on which that House has sat after the scheme is laid before it, the scheme shall be annulled accordingly, but without prejudice to the validity of anything previously done thereunder.

8. (1) The Minister may appoint to be members of the staff of the Commissioner such number of persons as may be determined from time to time by the Minister, with the consent of the Minister for Finance.

(2) Members of the staff of the Commissioner shall be public officers.

(3) The functions of the Commissioner under this Act may be performed during his temporary absence by such member of the staff of the Commissioner as he may designate for that purpose.

9. (1) The Commissioner shall keep in such form as may be approved of by the Minister, with the consent of the

Minister for Finance, all proper and usual accounts of all moneys received or expended by him and all such special accounts (if any) as the Minister, with the consent of the Minister for Finance, may direct.

(2) Accounts kept in pursuance of this paragraph in respect of each year shall be submitted by the Commissioner in the following year on a date (not later than a date specified by the Minister) to the Auditor-General for audit and, as soon as may be after the audit, a copy of those accounts, or of such extracts from those accounts as the Minister may specify, together with the report of the Auditor-General on the accounts, shall be presented by the Commissioner to the Minister who shall cause copies of the documents presented to him to be laid before each House of Parliament.

OBJECTS AND REASONS

The Bill seeks to provide a comprehensive framework for the protection of the privacy of personal information on individuals. It has been guided by the principles established under the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg in 1981, the Swiss Federal Law on Data Protection, the OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data, and the Data Protection laws of Ireland, the United Kingdom, Canada, Hong Kong and New Zealand.

The Bill also seeks to address concerns of the European Union regarding the transborder flow of personal data to jurisdictions with no or inadequate data protection legislation, and its stated intention to prohibit such flows from its member countries. The free flow of information across borders is the mainstay of the world economy. Without it the conduct of electronic business would be seriously compromised. It is therefore designed also to facilitate the international exchange of data by providing comparable levels of protection.

It is also important that individuals are assured that the information given, which sustains the information economy is appropriately protected against abuse and misuse.

The Bill applies data protection requirements to both the public and private sectors, although it allows for a transitional period for certain aspects of the legislation.

Clause 1 is the standard citation and commencement provision.

Clause 2 sets out the definition of terms used

in the Bill.

Clause 3 provides that the Crown is bound by the provisions of the Bill and stipulates the officers within government that may be designated data controllers and data processors for the purposes of the Bill.

Clause 4 sets out the application of the Bill.

Clause 5 sets out the exclusions to the Bill.

Clauses 6 and 7 provide that data must be collected lawfully and fairly and sets out the conditions under which personal data may be kept, including use of appropriate security measures to guard against unauthorised access to, alteration, disclosure, destruction or loss of data. This section incorporates the first five principles on data privacy under the OECD guidelines i.e. collection limitation, data quality, purpose specification, use limitation and security safeguards.

Clause 8 give effect to the OECD principle of individual participation which gives an individual the right to obtain data in relation to himself.

Clause 9 states the exceptions to this general right of access by individuals relating to national security concerns, crime prevention, tax and duty collections, financial fraud, professional legal privilege, statistics, research and detentions for law enforcement purposes, amongst others.

Clause 10 grants an individual the right to have inaccurate data rectified or erased.

Clause 11 grants an individual the right to prohibit the use of his personal data for the purpose of direct marketing.

Clause 12 sets out the duty of care owed by data controllers.

Clause 13 sets out the scope for disclosure of personal data in certain circumstances.

Clause 14 establishes the office and organisation of the Data Protection Commissioner.

Clause 15 endows the Commissioner with enforcement powers in relation to the administration of the Act.

Clause 16 provides for the issuance of enforcement notices by the Commissioner.

Clause 17 in keeping with the recommendations of both the OECD and the Council of Europe, grants the Commissioner the power to prohibit the transfer of personal data from the Bahamas to a jurisdiction that does not guarantee similar protections to that afforded under the Bill, in prescribed circumstances.

Clause 18 grants the Commissioner the power to require information in connection with any matters specified therein.

Clause 19 permits the Commissioner to appoint "authorised officers" for the purpose of obtaining information necessary for the purpose of administering the Bill.

Clause 20 provides for the approval of Codes of Practice prepared by and on behalf of data controllers. The mechanism for giving such codes, as approved, the force of law is also provided for.

Clause 21 provides for the Commissioner to prepare annual reports which are to be laid before each House of Parliament.

Clause 22 makes it an offence for a data processor to disclose personal data processed by him without the prior authorisation of the data controller, on whose behalf the data is being processed.

Clause 23 makes it an offence to disclose personal data obtained without authority.

Clause 24 sets out the procedure for appealing against a decision of the Commissioner.

Clause 25 allows for the use of certificates duly signed by the Minister, the Minister of National Security, the Commissioner of Police or the Commander of the Defence Force as evidence of the opinion of the respective official that disclosure of personal data is required for a prescribed purpose.

Clause 26 allows for the hearing of proceedings under the Bill to be heard in camera.

Clause 27 deals with the commission of offences by corporations.

Clause 28 deals with the conduct of proceedings for summary offences under the Bill.

Clause 29 sets out the maximum penalties to be applied on conviction for an offence under the Bill.

Clause 30 empowers the Minister to make regulations.

Clause 31 provides transitional arrangements allowing for a staggered implementation of certain requirements of the Act. This permits government agencies to continue to use data obtained prior to the coming into force of the Act for a five year period after its coming into force, howsoever such information may have been obtained. It also permits all data controllers and processors a grace period of one year after the Act comes into force to prepare their systems to respond to requests for access to information.