DATA PROTECTION BILL, 2008

(These notes form no part of the Bill but are intended only to indicate its general purport)

The Bill seeks to protect the privacy of personal and private information of individuals which is entered into electronic format.

The Bill would contain six Parts and ninety-nine sections.

Part I of the Bill would comprise the preliminary clauses and contains six clauses.

Clause 1 of the Bill would contain the short title and commencement.

Clause 2 of the Bill would provide for the interpretation of certain words and phrases.

Clause 3 of the Bill would bind the State.

Clause 4 of the Bill would set out the objects of the Act to ensure that protection is afforded to an individual's right to privacy and the right to maintain sensitive information as private and personal.

Clause 5 of the Bill would make the Bill inapplicable in respect of limiting information available by law to parties to proceedings, the power of a court or tribunal to compel witnesses to testify or produce documents and finally, personal notes in connection with proceedings prepared by or for persons presiding in a Trinidad and Tobago Court or tribunal.

Clause 6 of the Bill would establish the General Privacy Principles.

Part II of the Bill would provide for the office of the Data Commissioner and would contain twenty-two clauses.

Clause 7 of the Bill would establish the Office of the Data Commissioner.

Clause 8 of the Bill would empower the President to appoint a person to be the Data Commissioner who would be an attorney-at-law with at least 10 years standing at the bar and experience and training in economics, finance, information security, technology, audit or human resource management. The clause goes on to provide that the Data Commissioner when appointed would hold office for five years and may be reappointed. The Data Commissioner would be a corporation sole and is required to take and subscribe to an oath of office.

Clause 9 of the Bill would set out the powers of the Data Commissioner which include *inter alia* conducting audits and investigations to ensure compliance with the Act,

ordering a public authority to cease collection practices or destroy collections of personal information that contravenes the Act and authorizing data matching by public authorities.

Clause 10 of the Bill would set out the functions of the Data Commissioner which include *inter alia* promoting the development of codes of conduct, promoting the adherence to good practices, disseminating information about the Act and monitoring compliance with the Act.

Clause 11 of the Bill would empower the President to also appoint a Deputy Data Commissioner to act in the absence of the Data Commissioner who would hold office for five years and have the same qualifications and experience as the Data Commissioner. The clause also empowers the President to appoint an acting Deputy Data Commissioner in the absence of the Deputy Data Commissioner.

Clause 12 of the Bill would provide for the removal, or resignation of the Data Commissioner and Deputy Data Commissioner for cause including misconduct in relation to his duties or physical or mental inability to perform the responsibilities of the office of Data Commissioner. The clause also provides that the Data Commissioner may resign by letter addressed to the President.

Clause 13 of the Bill would provide that both the Corporation and the Deputy Data Commissioner would enjoy the terms and conditions of a High Court Judge.

Clause 14 would provide for the seal of the Data Commissioner and the use of the seal.

Clause 15 of the Bill would provide for the location of the Office of the Data Commissioner for the service of documents.

Clause 16 of the Bill would provide for the execution of documents by the Data Commissioner.

Clause 17 of the Bill would provide for staff of the Office of the Data Commissioner to be public officers or persons employed by the Data Commissioner as consultants, mediators or such other persons necessary to enable him to perform the duties of the Office of Data Commissioner. The clause provides for the preservation of rights of public officers who are seconded and the period of such secondment. Public officers may also be transferred to the office of the Data Commissioner. The clause would also set out provisions for pensions for employees.

Clause 18 of the Bill would empower the Data Commissioner to delegate to any person any of his powers, duties or functions subject to limitations or restrictions which he determines necessary, but only permits the Data Commissioner to delegate his responsibilities in respect of disclosures under sections 24 to 26 of the Freedom of Information Act to the Deputy Data Commissioner.

Clause 19 of the Bill would provide for the designation and powers of inspectors.

Clause 20 of the Bill would set out the powers of the Data Commissioner when he is conducting an audit or inquiry into the practices of a public authority or where he is determining an appeal pursuant to the principles set out in Part III. The clause goes on to prohibit the retention of any information obtained from data under this clause. The clause also requires the Data Commissioner to notify the head of a public authority before entering the premises of his purpose for so entering. The clause goes on to set out the circumstances under which the Data Commissioner is required to exercise his powers under this clause.

Clause 21 of the Bill would set out the powers of the Data Commissioner where he is conducting an audit or inquiry pursuant to Part IV. These include the power to require the production of documents, enter and inspect premises and summon and examine persons under oath. The clause however prohibits the Data Commissioner from retaining any information obtained from data received under this clause.

Clause 22 of the Bill would provide for the accounts and expenses of the office of the Data Commissioner.

Clause 23 of the Bill would provide that statements which are made to the Data Commissioner are not admissible as evidence in court or any other proceedings except where it is in a prosecution for perjury in respect of sworn testimony or for an offence under this Act or where in an application for judicial review or an appeal, for a decision in respect of that application.

Clause 24 of the Bill would provide that any thing said in information supplied or any data produced during an investigation by the Data Commissioner is privileged.

Clause 25 of the Bill would restrict the Data Commissioner in respect of the disclosure of information which he receives during the performance of his duties.

Clause 26 of the Bill would give the Data Commissioner or any person acting for or under his direction immunity from suit for anything done, reported or said in good faith during the performance of their duties.

Clause 27 of the Bill would require the Data Commissioner to submit a report yearly to Parliament on the activities of his office and may be required to submit special reports to Parliament periodically where such reports are required.

Clause 28 of the Bill would require the Data Commissioner to publish by Order, a list of countries which have comparable safeguards as provided by this Act, for personal data.

Part III of the Bill would provide for the protection of personal data by Pubic Authorities and would contain thirty-nine clauses.

Clause 29 of the Bill would provide for the interpretation of personal information as it is used in the Act.

Clause 30 of the Bill would limit a public authority's collection of personal information to that which is authorized by law, law enforcement and where the information is directly related to an operating programme or activity of the public authority.

Clause 31 of the Bill would require that personal information be collected directly from the individual except in certain circumstances.

Clause 32 of the Bill would require a public authority to inform a person from whom it collects personal information as to why it is being collected, the legal authority for collecting it, and the title, business address and business phone number of an official who can answer questions about the collection. The clause goes on to provide, in certain circumstances, an exception to this requirement to provide information.

Clause 33 of the Bill would require a public authority to retain personal information it has used for a period of time as is prescribed by the Minister by Order.

Clause 34 of the Bill requires a public authority where it intends to use personal information to make a decision that would affect the individual to ensure that the information is correct and complete.

Clause 35 of the Bill would require a public authority to keep all personal information secure, arrangements against unauthorized access, collection, use, alteration, disclosure or disposal of personal information.

Clause 36 of the Bill would require personal information held by a public authority be stored and accessed only in Trinidad and Tobago except where the consent is given by the individual to whom the information relates, to it being stored or accessed outside of Trinidad and Tobago or where it is stored or accessed outside of Trinidad and Tobago from a jurisdiction that has comparable safeguards as provided by this Act.

Clause 37 of the Bill would require a public authority to dispose of all personal information in its control or custody in accordance with regulations made by the Minister under this Act.

Clause 38 of the Bill would prohibit a public authority which has custody and control of personal information from use of such information except for the purposes for which it was obtained unless it has the consent of the individual.

Clause 39 of the Bill would provide for what is meant by information being used consistent with the purpose for which it was obtained or compiled.

Clause 40 of the Bill would limit the processing of sensitive personal information in the possession of a public authority.

Clause 41 of the Bill would prohibit the disclosure of personal information in Trinidad and Tobago by a public authority without the consent of the individual in respect of whom the information relates except in certain circumstances. The clause goes on to require that the public authority must, before divulging information of a party residing in another jurisdiction, inform the individual to whom the information relates of the identity of the relevant statutory authority in the other jurisdiction.

Clause 42 of the Bill would set out the circumstances under which personal information may be disclosed.

Clause 43 of the Bill would empower a public authority to disclose personal information for statistical and research purposes in certain circumstances.

Clause 44 of the Bill would empower a public authority to disclose personal information for archival or historical purposes in certain circumstances.

Clause 45 would restrict the disclosure of medical information.

Clause 46 of the Bill would provide for the disclosure of personal information outside of Trinidad and Tobago.

Clause 47 of the Bill would require Government Ministries to prepare a privacy impact assessment in respect of any new enactment, system, project, programme or activity and would set out the consequential requirements on each Ministry thereafter.

Clause 48 of the Bill would require the head of a public authority to place all personal information in its custody and control in personal information banks. Personal information in the custody and control of the Archives of Trinidad and Tobago are exempt from this clause.

Clause 49 of the Bill would require a public authority where it intends to share information with other public authorities to do so in a form approved by the Data Commissioner.

Clause 50 of the Bill would require a public authority to obtain the written authorization of the Data Commissioner before matching personal information with other data. The clause goes on to empower the Data Commissioner to give covering authorization where a system of practice has developed.

Clause 51 of the Bill would require the Minister to publish an index of personal information that is held by public authorities and sets out what such index should contain.

Clause 52 of the Bill would give every resident or citizen of Trinidad and Tobago the right to access his personal information that is contained in a personal information bank and any other personal information which is in the custody or control of a public authority.

Clause 53 of the Bill would empower a public authority to refuse to disclose personal information to the individual to whom the information relates in certain circumstances

Clause 54 of the Bill would empower the head of a public authority to which a request has been made for personal information under section 52 to sever the information which is exempt from disclosure under section 53 and furnish the remaining information. The head of the public authority may, where the disclosure about the existence of exempt information reveal the contents of such exempt information, refuse to disclose the existence of such exempt information.

Clause 55 of the Bill would provide for the manner by which the personal information of deceased persons is to be treated.

Clause 56 of the Bill would set out the responsibilities of public authorities where a request is made for personal information.

Clause 57 of the Bill would entitle an individual in respect of whom personal information is held by a public authority and which the individual believes to be incorrect, to request the correction of such personal information. The obligations on the public authority thereafter are also set out.

Clause 58 of the Bill would entitle an individual who has been refused access to personal information, who makes a request under the Freedom of Information Act or who has requested personal information be corrected to appeal from the decision of the public authority to the Data Commissioner.

Clause 59 of the Bill would provide that an appeal to the Data Commissioner is to be made within six weeks of the date on which the notice was given of the decision.

Clause 60 of the Bill would empower the Data Commissioner to dismiss an appeal immediately where the notice of appeal does not present a reasonable basis for concluding that the personal information exist.

Clause 61 of the Bill requires the Data Commissioner to inform the head of the public authority concerned and any other affected person of the notice of appeal.

Clause 62 of the Bill empowers the Commissioner to authorize a mediator to investigate the circumstances of the appeal with the intention of settling the matter.

Clause 63 of the Bill would empower the Data Commissioner to conduct an enquiry to review the decision of the head of a public authority where the Data Commissioner had not authorized a mediator to conduct an investigation or where he has so authorized but there is no settlement.

Clause 64 of the Bill would provide for the enquiry by the Data Commissioner or the mediator to be conducted in private.

Clause 65 of the Bill would entitle the person who requested access to personal information, the head of the public authority and any affected party to make representations to the Data Commissioner but does not entitle such person to be present during the presentations of other persons before the Data Commissioner.

Clause 66 of the Bill would entitle the person who requested access to personal information, the head of the public authority and any affected party to be represented by counsel or an agent.

Clause 67 of the Bill shifts the burden of proof on the balance of probabilities that the information lies within one of the specified exemptions of the Act to the public authority where it refuses access to personal information.

Part IV of the Bill would provide for the protection of personal information by the private sector and contains seventeen clauses.

Clause 68 of the Bill requires persons who collect and store personal information to follow the General Privacy Principles in section 6.

Clause 69 of the Bill would require the Data Commissioner to consult with industry for the development of codes of practice.

Clause 70 of the Bill would empower the Data Commissioner where in his opinion, the public interest so warrants, to require the development of mandatory codes of conduct for particular industries, sectors or activities.

Clause 71 would provide for cross-border disclosure of personal information.

Clause 72 would empower the Data Commissioner to approve a code of conduct developed by an industry sector, an industry organization, a professional body, or any other person who applies to the Data Commissioner for such approval.

Clause 73 would empower the Minister where the Data Commissioner approves a code of conduct to make the code legally enforceable by Order or Regulations.

Clause 74 of the Bill would limit the processing of sensitive personal information in the possession of a corporation.

Clause 75 of the Bill would provide for the refusal of a request for access to personal information and the notification of such refusal.

Clause 76 of the Bill would allow an individual aggrieved by the actions of an organization, which is subject to a mandatory code in respect of his personal information

and which is in the custody and control of the organization to request the Data Commissioner to conduct a review of the decision, act or failure to act of the organization or make a complaint to the Data Commissioner in respect of the organisation's failure to comply with the mandatory code of conduct.

Clause 77 of the Bill would set out the timeframe for an application for a review or a complaint.

Clause 78 would empower the Data Commissioner to dismiss a request for a review or a complaint in certain circumstances.

Clause 79 would require the Data Commissioner to notify the head of an organization where a request has been made for a review of a decision of the organization or where a complaint has been made against such organization.

Clause 80 would empower the Commissioner to conduct an enquiry into a request or complaint.

Clause 81 would empower the Commissioner to authorize a mediator to investigate the circumstances of the request.

Clause 82 would provide that where the inquiry is held by the Commissioner or mediator or any meetings are to be held in respect of a request the inquiry or the meeting should be conducted in private.

Clause 83 would provide that a person requesting access to personal information or the head of the organization concerned may make representation to the Commissioner.

Clause 84 of the Bill would impose duties on directors and officers of a corporation.

Part V of the Bill would set out the offences under this Act and contains ten clauses.

Clause 85 of the Bill makes it an offence if a person wilfully obstructs the Data Commissioner or any other person acting for or under his direction while carrying out an audit or an investigation. The clause goes further to provide that if a director of officer is found guilty of such offence he is liable to a fine of five hundred thousand dollars.

Clause 86 of the Bill makes it an offence for a person to make a request for information under false pretences. The clause also makes it an offence where a person wilfully makes a false statement to mislead or attempts to mislead the Data Commissioner in the performance of his functions.

Clause 87 of the Bill makes it an offence for a person to fail to comply with an order of the Commissioner.

Clause 88 of the Bill makes it an offence for any person who contravenes section 98 which deals with whistle-blowers.

Clause 89 would make it an offence for non-compliance with a mandatory code under section 73.

Clause 90 of the Bill makes it an offence for a person to wilfully disclose information or maintain a personal information bank in contravention of this Act.

Clause 91 of the Bill would make it an offence for a person to breach the confidentiality obligations under section 25.

Clause 92 of the Bill would provide that where a corporation commits an offence under this Act, its officers, directors or agents who directed, authorized, assented to, acquiesced in or participated in the commission of the offence is party to and commits an offence and would be liable to the punishment provided for the offence whether or not the corporation has been prosecuted or convicted.

Clause 93 of the Bill would set out the penalties for offences under this Act ranging from fifty thousand dollars to five hundred thousand dollars.

Clause 94 would set out the penalties for corporations.

Part VI of the Bill would set out miscellaneous provisions and contain five clauses.

Clause 95 of the Bill would provide for the payment of the cost of an audit performed under sections 20 and 21.

Clause 96 of the Bill would set out the jurisdiction of the court under this Act.

Clause 97 would grant protection for persons who divulge information about breaches of this Act in their organization. An employer would therefore be prohibited from dismissing, suspending, demoting, disciplining, harassing or otherwise disadvantaging an employee or denying the employee of any benefit.

Clause 98 of the Bill would empower the Minister to make regulations for the purpose of giving effect to the requirements of this Act. The regulations will be subject to negative resolution of Parliament.

Clause 99 would make consequential amendments to the Freedom of Information Act, Chap. 22:02.

THE DATA PROTECTION BILL, 2008

Arrangement of Clauses

Clause

PART III
PROTECTION OF PERSONAL DATA BY PUBLIC AUTHORITIES

PART IV
PROTECTION OF PERSONAL DATA BY THE PRIVATE SECTOR

PART V
CONTRAVENTION AND ENFORCEMENT

PART VI
MISCELLANEOUS

A Bill

An Act to provide for the protection of personal privacy and information

Enactment. ENACTED by the Parliament of Trinidad and Tobago as follows:

PART I
PRELIMINARY

Short title and commencement.

1.(1) This Act may be cited as the Data Protection Act, 2008.

(2) This Act shall come into operation on such day as is fixed by the President by Proclamation and different days may be fixed for different provisions of this Act.

Interpretation.

2. In this Act-

"Commissioner" means the Data Commissioner appointed under section 8;

"contact information" means information to enable an individual or business to be contacted and includes in respect of the representative of a business, his personal phone number and address and in respect of the business, the name, position name or title, business telephone number, business address and business e-mail and facsimile number of the individual;

"Corporation" means the corporation sole established under section 8(3);

"Court" means the High Court of Trinidad and Tobago;

"data" means any document, correspondence, memorandum, book, plan, map, drawing, pictoral or graphic work, photograph, film, microfilm, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy of those things;

"data matching" means the comparison, whether naturally or by means of any electronic or other device, of any data that contains personal information about

individuals with other documents containing personal information about individuals for the purpose of producing new forms of information about individuals;

"enterprise" means a partnership or body (corporate or unincorporated) engaged in business;

"head of a public authority" means the Permanent Secretary of a Ministry, the Head of a Government Department, President or Chief Executive Officer of a corporation or the Chairman of an agency;

"health care body" means a regional health authority established under the Regional Health Authorities Act, a hospital, extended care facility, clinic, Psychiatric Hospital as defined under Mental Health Act, a private hospital as defined under the Private Hospitals Act, and similar bodies licensed by the Minister with responsibility for health;

Chap. 29:05

Chap.28:02

Chap. 29:03

"individual" means a natural person;

"information sharing agreement" means an agreement that sets conditions for one or more of the following:

(a) the exchange of personal information between a public authority and a person, a group of persons or an organization;

(b) the disclosure of personal information by a public authority to a person, a group of persons or an organization; or

(c) a collection of personal information by a public authority from a public authority, a person or a group of persons of an organization;

"Minister" means the Minister to whom responsibility for data protection is assigned and "Ministry" shall be construed accordingly;

"personal information" means information about an identifiable individual that is recorded in any form including-

(a) information relating to the race, national or ethnic origin, religion, age or marital status of the individual;

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to the financial transactions in which the individual has been involved or which refers to the individual;

(c) any identifying number, symbol or other particular designed to identify the individual;

(d) the address, fingerprints, Deoxyribonucleic Acid or blood type of the individual;

(e) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual;

(f) correspondence sent to an establishment by the individual that is explicitly or implicitly of a private or confidential nature, and relies on such correspondence which would reveal the contents of the original correspondence; or

(g) the views and opinions of any other person about the individual;

"personal information bank" means a collection of personal information that is organized or retrievable by the name of the individual or by an identifying number, symbol or other particulars assigned to the individual;

"privacy impact assessment" means an assessment that is conducted to determine if a proposed enactment, system, project, programme or activity meets the requirements of the General Privacy Principles of section 6;

"public authority" means –

(a) Parliament, a Joint Select Committee of Parliament or a committee of either House of Parliament;

(b) the Court of Appeal, the High Court, the Industrial Court, the Tax Appeal Board or any court of summary jurisdiction;

(c) the Cabinet as constituted under the Constitution, a Ministry or Department, Division or Agency of a Ministry;

(d) the Tobago House of Assembly, the Executive Council of the Tobago House of Assembly or a division of the Tobago House of Assembly;

Chap. 25:04

(e) a municipal corporation established under the Municipal Corporations Act;

(f) a statutory body, responsibility for which is assigned to a Minister of Government;

(g) a company incorporated under the laws of Trinidad and Tobago that is owned and controlled by the State;

(h) a Service Commission established under the Constitution or other written law; or

(i) a body corporate or unincorporated entity in relation to any function that it exercises on behalf of the State, or which is supported, directly or indirectly by Government funds and over which Government is in a position to exercise control;

"sensitive personal information" means personal information on a person's –

(a) racial or ethnic origins;

(b) political opinions;

(c) religious beliefs or other beliefs of a similar nature;

(d) physical or mental health or condition;

(e) sexual orientation or sexual life; or

(f) criminal or financial record;

"sensory disability" means a disability that relates to sight or hearing; and

"service provider" means a person retained under a contract to perform services of a public authority.

Act binds the State.

3. This Act binds the State.

Object of Act.

4. The object of this Act is to ensure that protection is afforded to an individual's right to privacy and the right to maintain sensitive personal information as private and personal.

Inapplicability of Act.

5. This Act shall not-

(a) limit information available by law to a party in any proceeding;

(b) limit the power of a court or tribunal to compel a witness to testify or to compel the production of a document or other evidence; or

(c) apply to notes prepared by or for an individual presiding in a court of Trinidad and Tobago or in a tribunal if those notes are prepared for that individual's personal use in connection with the proceedings.

General Privacy Principles.

6. The following principles are the General Privacy Principles which are applicable to all persons who handle, store or process personal information belonging to another person:

(a) an organization shall be responsible for the personal information under its control;

(b) the purpose for which personal information is collected shall be identified by the organization before or at the time of collection;

(c) knowledge and consent of the individual are required for the collection, use or disclosure of personal information;

(d) collection of personal information shall be legally undertaken and be limited to what is necessary in accordance with the purpose identified by the organization;

(e) personal information shall only be retained for as long as is necessary for the purpose collected and shall not be disclosed for purposes other than the purpose of collection without the prior consent of the individual;

(f) personal information shall be accurate, complete and up-to-date as is necessary for the purpose of collection;

(g) personal information is to be protected by such appropriate safeguards necessary in accordance with the sensitivity of the information;

(h) sensitive personal information is protected from processing except where otherwise provided for by written law;

(i) organizations are to make available to individuals documents regarding their policies and practices related to the management of personal information except where otherwise provided by written law;

(j) organizations shall, except where otherwise provided by written law, disclose at the request of the individual, all documents relating to the existence, use and disclosure of personal information, such that the individual can challenge the accuracy and completeness of the information;

(k) the individual has the ability to challenge the organization's compliance with the above principles and receive timely and appropriate engagement from the organization; and

(l) personal information which is requested to be disclosed outside of Trinidad and Tobago shall be regulated and comparable safeguards to those under this Act shall exist in the jurisdiction receiving the personal information.

PART II

OFFICE OF THE DATA COMMISSIONER

Office of the Data Commissioner.

7. There is hereby established a body to be known as the Office of the Data Commissioner.

Appointment of Data Commissioner.

8.(1) There shall be a Data Commissioner who shall be the head of the Office of the Data Commissioner and who shall be appointed by the President and who shall possess the qualifications and experience set out in subsection (2).

(2) A person appointed to be the Data Commissioner under

subsection (1) shall be an attorney-at-law within the meaning of the Legal Profession Act with at least ten years standing at the bar and shall have training or experience in economics, finance, information security, technology, audit or human resource management.

Chap. 7:07

(3) The Data Commissioner shall be a corporation sole.

(4) A person appointed under subsection (1) shall hold office for five years and may be reappointed.

(5) A person appointed under subsection (1) shall, before he performs the functions of Data Commissioner, take and subscribe to the oath of office set out in the Schedule.

Schedule

Powers of Data Commissioner.

9.(1) The Commissioner shall monitor the administration of this Act to ensure its purposes are achieved.

(2) In carrying out his powers under subsection (1), the Commissioner may-

(a) conduct audits and investigations to ensure compliance with any provision of this Act;

(b) offer comment on the privacy protection implications of proposed legislative schemes or government programmes and receive representations from the public concerning data protection and privacy matters;

(c) after hearing the representations of the head of a public authority or an organization subject to a mandatory code of conduct and who may be engaged in processes that may be in contravention of this Act, order the public authority or organization to cease collection practices or destroy collections of personal information that contravene this Act;

(d) authorize the collection of personal information otherwise than directly from the individual in appropriate circumstances;

(e) make orders regarding the reasonableness of fees required by an organization subject to this Act;

(f) authorize data matching by a public authority or public authorities;

(g) make orders, including such terms and conditions as the Commissioner considers appropriate, following an appeal or complaint filed by an individual pursuant to section 58 or 76;

(h) make orders regarding compliance with the General Privacy Principles set out in section 6 by a public authority or an organization subject to a mandatory code of conduct;

(i) hold such property as is by this Act vested in him, as well as such property as may from time to time-

(i) by virtue of any other written law; or

(ii) in any other way,

be or may become vested in him;

(j) with the permission of the President acquire, purchase, take, hold and enjoy movable and immovable property of every description, convey, assign, surrender and yield up, mortgage, demise, re-assign, transfer or otherwise dispose of, or deal with any movable or immovable property vested in the Commissioner upon such terms as the Commissioner seems fit;

(k) accept surrenders, assignments or re-conveyances and to exchange any property and enter into contracts;

(l) publish guidelines regarding compliance with the Act, including but not limited to guidelines on the development of industry codes of conduct, firm compliance policies, procedures for handling complaints, guidelines dealing with conflict of interest for industry bodies or individuals who mediate or deal with complaint resolution, guidelines dealing with security of information and information systems, and guidelines for information sharing agreements or data matching agreements;

(m) exercise his corporate powers in relation thereto in such manner as he thinks fit, subject always to any special or general directions as the President may from time to time specify; and

(n) exercise such other powers as may be assigned to him under any other written law.

Functions of Data Commissioner.

10. The Commissioner appointed under section 8 shall-

(a) promote the development of codes of conduct for guidance as to good practice;

(b) promote the adherence to good practices by persons subject to this Act;

(c) disseminate information about this Act;

(d) monitor compliance with this Act;

(e) co-operate with counterparts in other jurisdictions to promote the protection of personal privacy in the public and private sectors;

(f) carry out special studies or research regarding privacy or related issues either upon his own initiative or upon the request of the President;

(g) bring to the attention of the head of the public authority or organization subject to a mandatory code of conduct any failure to meet the standards imposed by the General Privacy Principles set out in section 6 or the responsibilities established by Part III and Part IV of this Act;

(h) issue public reports on the status of compliance with this Act;

(i) review and approve privacy impact assessments as required by this Act; and

(j) exercise such other functions that may be assigned to him under any other written law.

Deputy Data Commissioner.

11.(1) There shall be a Deputy Data Commissioner who shall be appointed by the President and who shall possess the same qualifications and experience required for the Data Commissioner under section 8.

(2) The Deputy Data Commissioner shall hold office for five years and may be reappointed.

(3) The Deputy Data Commissioner may in the absence or incapacity of the Data Commissioner act in his place.

(4) Where the post of Data Commissioner is vacant the Deputy Data Commissioner may act as the Data Commissioner until such time as a Data Commissioner is appointed to the vacant post.

(5) In the absence or incapacity of the Deputy Data Commissioner, the President may appoint an acting Deputy Data Commissioner.

Resignation, removal and suspension of Data Commissioner and Deputy Data Commissioner.

12.(1) The Commissioner or Deputy Data Commissioner may be removed from office only for cause, including misconduct in relation to his duties or physical or mental inability to fulfil the responsibilities of the office.

(2) The Commissioner or Deputy Data Commissioner may at any time resign his office by letter addressed to the President.

Remuneration of Data Commissioner and Deputy Data Commissioner.

13. Section 141 of the Constitution shall apply to the offices of the Commissioner and the Deputy Data Commissioner.

Seal of Corporation.

14. (1) The Corporation shall have a seal which shall be kept in the custody of the Commissioner and shall be judicially noticed as such.

(2) The seal of the Corporation may be affixed to documents and instruments in the presence of the Commissioner and shall be attested by the signature of the Commissioner and the signature shall be sufficient evidence that the seal was duly and properly affixed and is the lawful seal of the Corporation.

(3) All documents, other than those required by law to be under seal made by, and all decisions of the Corporation may be signified under the hand of the Commissioner.

(4) Notwithstanding the provisions of the Conveyancing and Law of Property Act and the Real Property Act relating to the matters thereunder required to be performed and to the mode of their performance prior to the registration of a Deed, document or other instrument, the affixing of the seal of the Corporation and the signing by the Commissioner in the manner set out in subsection (2) shall be, and shall be taken as, sufficient evidence for the purposes of those Acts of the due execution by the Corporation of any Deed, document or other instrument.

Chap. 56:01

Chap. 56:02

Location of Office of Data Commissioner and service of documents.

15.(1) The office of the Corporation shall be situated at the Office of the Data Commissioner.

(2) Service upon the Commissioner of any notice, order or other document shall be effected by delivering the same or by sending it by registered post addressed to the Commissioner at the office of the Corporation.

Execution of documents.

16. (1) Any document required to be executed by the Corporation shall be deemed to be duly executed if signed—

(a) by the Commissioner; or

(b) outside Trinidad and Tobago by the person or persons authorized by the Commissioner so to sign, but in such case the instrument so authorizing such person or persons shall be attached to and form part of the document.

(2) Any cheque, bill of exchange or order for the payment of money required to be executed by the Commissioner shall be deemed to be duly executed if signed by a person or persons authorized to do so by the Commissioner.

Staff of the Office of Data Commissioner.

17.(1) The Commissioner may employ such persons as he considers necessary for the due and efficient performance of his duties and functions under this Act on such terms and conditions as are agreed between the Commissioner and the person and subject to such maximum

limit of remuneration as the Minister may determine.

(2) Subject to subsection (3) and the approval of the appropriate Service Commission or Statutory Authority and with the consent of the officer, any officer in the public service or a Statutory Authority may be seconded to the service of the Office of the Data Commissioner.

(3) Where a secondment referred to in subsection (2) is effected, arrangements shall be made to preserve the rights of the officer so transferred to any pension, gratuity or other allowance for which he would have been eligible had he not been seconded to or from the service of the Office of the Data Commissioner.

(4) A period of transfer on secondment shall be for three years and may only be extended for a further two years.

(5) Subject to the approval of the Commissioner, the appropriate Service Commission and with the consent of the officer, an officer in the public service or a Statutory Authority may be transferred to the service of the Office of the Data Commissioner on terms and conditions no less favourable than those enjoyed by the officer at the time of transfer in the public service or Statutory Authority, as the case may be.

(6) The Commissioner shall establish a pension fund plan, or where the establishment of a plan is not feasible, the Commissioner shall make arrangements for membership in a pension plan, join an existing plan.

(7) Subject to the rules of the pension plan established in accordance with subsection (6), all employees of the Office of the Data Commissioner shall be eligible to become members of the pension fund plan established in accordance with subsection (6).

(8) Superannuation benefits which had accrued to a person

transferred in accordance with subsection (5) shall be preserved as at the date of his employment by the Commissioner and such benefits shall continue to accrue under the relevant pension law up to the date of establishing a pension plan for the date on which arrangements are made for membership in a plan on the basis of pay, pensionable emoluments or salary, as the case may be, applicable, at the time of this transfer, to the office held by him immediately prior to his employment by the Commissioner.

(9) Where a person who is transferred in accordance with subsection (5) dies, retires or his post in the Office of the Data Commissioner is abolished or he is retrenched by the Commissioner prior to establishing or prior to the arrangements being made for membership in a pension plan and, if at the date that his service is terminated by any of the above-mentioned methods he was in receipt of a salary higher than the pay, pensionable emoluments or salary referred to in subsection (8), the superannuation benefits payable to his estate or to him, as the case may be, shall be based on the higher salary.

(10) The difference between the superannuation benefits payable on the basis of the higher salary referred to in subsection (9) and the superannuation benefits payable under the relevant pension law, on the basis of the pay, pensionable emoluments or salary, referred to in subsection (8), shall be paid by the Commissioner.

(11) Where a person who is transferred in accordance with subsection (5) dies, retires or his post in the Office of the Data Commissioner is abolished or he is retrenched from the Office of the Data Commissioner while being a member of the pension fund plan established in accordance with subsection (6), he shall be paid superannuation benefits by the pension fund plan at the amount which, when combined with superannuation benefits payable under the relevant pension law, is equivalent to the benefits based on his pensionable

service in the public service or a Statutory Authority combined with his service in the Office of the Data Commissioner and calculated at the final salary applicable to him on the date that his service was terminated by any of the above-mentioned methods.

(12) For the purpose of subsection (11) "final salary" shall have the meaning assigned to it by the pension fund plan.

Delegation.

18.(1) Subject to subsection (2), the Commissioner may authorize any person to exercise or perform, subject to such restrictions or limitations as the Commissioner may specify, any powers, duties or functions of the Commissioner.

(2) The Commissioner may delegate to only the Deputy Data Commissioner responsibilities regarding review of personal information that deals with matters that may be exempt from disclosure pursuant to sections 24 to 26 of the Freedom of Information Act.

Chap. 22:02

Designation and powers of inspectors.

19.(1) The Minister may designate public officers to be inspectors according to their qualifications for the purposes of this Act and shall furnish each such inspector with a certificate of his designation.

(2) Where the Commissioner is conducting an enquiry or inspection under this Act the officers appointed under subsection (1) shall act on his behalf.

(3) An inspector shall, subject to sections 20 and 21 have the power to do all or any of the following things for the purpose of the execution of this Act:

(a) if he considers necessary, take with him when entering any vehicle, land or premises, a police officer;

(b) to require the production of or to seize, inspect or examine and to copy registers, records or other documents;

(c) to make such examinations, inspections, investigations and enquiries as may be necessary to ascertain whether this Act is being complied with;

(d) to require any person whom he finds in such vehicle or on such land or premises to give such information as is in his power to give as to who is the owner or occupier thereof and the employer of workers employed to work thereon;

(e) to examine, either alone or in the presence of any other person as the inspector thinks fit, with respect to the observance of the provisions of this Act or the Regulations, any person whom he finds in such vehicle or on such land or premises or whom he has reasonable cause to believe to be, or to have been within the preceding two months, employed thereon, and to require any such person to be so examined and to sign a declaration of the truth of the matters respecting which he is so examined; so, however, that no person shall be required under this provision to answer any question or to give evidence tending to incriminate himself; and

(f) to seize and detain for such time as may be necessary any article by means of which, or in relation to which he reasonably believes any provision of this Act has been contravened.

Power of Commissioner to conduct an audit or enquiry of a public authority pursuant to Part III.

20.(1) Where the Data Commissioner is conducting an audit or enquiry into the practices of a public authority for the purposes of ensuring compliance with the General Privacy Principles set out in Part I, or determining an appeal pursuant to Part III, the Commissioner may-

(a) with the permission of the head of the public authority or on application for a warrant under subsection (4), enter and inspect any premises occupied by a public authority for the purposes of an audit or enquiry;

(b) require the production of any document or record relevant to the enquiry that is in the custody or control of a public authority.

(2) The Commissioner shall not retain any information obtained from an audit or enquiry under subsection (1) beyond the period for which it is required.

(3) The Commissioner may exercise his powers under this section with respect to Parliament, a Joint Select Committee of Parliament or a committee of either House of Parliament, the Cabinet, the Court of Appeal, the High Court, the Industrial Court, the Tax Appeal Board or any court of summary jurisdiction, the Tobago House of Assembly, the Executive Council of the Tobago House of Assembly only with the consent of the Speaker of the House or the President of the Senate, the Head of the Cabinet, the Chief Justice, the Presiding Officer or the Head of the Executive Council as the case may be.

(4) Where the head of a public authority refuses to-

(a) allow the Data Commissioner or any person acting for or under him to enter and inspect premises under subsection (1)(a), the Data Commissioner shall, where he believes that such entry is necessary, apply to a Magistrate for a warrant to so enter and inspect; or

(b) produce a document or record under subsection (1)(b), the Data Commissioner shall, where he believes the request to be reasonable, apply to the Court for an Order requiring the public authority to produce such documents.

(5) Subsection (4) shall not apply to any authority referred to in subsection (3).

Power of Commissioner to conduct audit or enquiry pursuant to Part IV.

21.(1) Where the Commissioner is conducting an audit or enquiry into the compliance practices of a person subject to the provisions of an enforceable code of conduct pursuant to Part IV of this Act, the Commissioner may, pursuant to the authority provided under subsection (2) by –

(a) an Order of the Court, require the production of any document or record that is in the custody or control of a person subject to an enforceable code of conduct; or

(b) a warrant, enter and inspect any premises occupied by a person subject to an enforceable

code of conduct for the purposes of an audit or enquiry.

(2) Where a private enterprise refuses to allow the Data Commissioner or any person acting for or under him to enter and inspect premises under subsection (1)(a), the Data Commissioner may apply to a Magistrate for a warrant to so enter and inspect; or

(3) Where a private enterprise refuses to produce a document or record under subsection (1)(b), the Data Commissioner may apply to the Court for an Order requiring the public authority to produce such documents.

(4) The Commissioner shall not retain any information obtained from an audit or enquiry under subsection (1) beyond the period for which it is required.

Expenses and accounts of the Office of the Data Commissioner.

22.(1) All expenses of the Office of the Data Commissioner shall be met out of moneys provided by Parliament.

(2) All revenues of the Office of the Data Commissioner shall be paid into the Consolidated Fund.

(3) The accounts of the Office of the Data Commissioner shall be audited by the Auditor General in accordance with the provisions of the Exchequer and Audit Act.

Chap. 69:01

Statements made to Commissioner not admissible.

23. A statement made to or an answer given by a person during an investigation or enquiry by the Commissioner is inadmissible as evidence in court or any other proceeding, except in -

(a) a prosecution for perjury in respect of sworn testimony;

(b) a prosecution for an offence under this Act; or

(c) an application for judicial review or an appeal from a decision with respect to that application.

Privileged information.

24. Anything said in information supplied or any data produced by a person during an investigation or enquiry by the Commissioner is privileged in the same manner as if the investigation or enquiry were a proceeding in a court.

Restrictions on disclosure of information by Commissioner and staff.

25.(1) The Commissioner and anyone acting for or under the direction of the Commissioner shall not disclose any information obtained in performing their duties, powers and functions under this Act.

(2) Notwithstanding subsection (1), the Commissioner may disclose or may authorize anyone acting for or under the direction of the Commissioner, to disclose information -

(a) necessary to conduct an investigation, audit or enquiry under this Act or establish grounds for findings and recommendations contained in a report under the Act; or

(b) in the course of a prosecution or an appeal from, or judicial review of a decision, of the Commissioner.

Protection of Commissioner and staff.

26. Proceedings shall not lie against the Commissioner or a person acting for or under the direction of the Commissioner for anything done, reported or said in good faith in the exercise or performance or the intended exercise or performance of a duty, power or function under this Part.

Annual report of Commissioner.

27.(1) The Commissioner shall submit a report annually to Parliament on the activities of the Office of the Data Commissioner for the previous year commencing one year after the coming into operation of this Act.

(2) The Commissioner may submit a special report to Parliament at any time commenting on any matters within the scope, duties and functions of the Commissioner where the matter is of such urgency or importance that it should not be deferred to the time of the

next annual report to Parliament.

Commissioner to publish list of equivalent jurisdictions.

28. The Data Commissioner shall by Order publish a list of countries which have comparable safeguards for personal information as provided by this Act.

PART III

PROTECTION OF PERSONAL DATA BY PUBLIC AUTHORITIES

Personal information.

29.(1) The following information about an individual who is or has been an employee or official of a public authority is not personal information for the purpose of this Act –

(a) the fact that the individual is or has been an employee or official of a public authority;

(b) the title, business address and telephone number of the individual;

(c) the name of the individual on a document prepared by the individual in the course of employment; and

(d) the professional opinions or views of the individual given in the course of employment.

(2) Information about an individual who is or was performing services under contract for a public authority that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services is not personal information for the purposes of the Act.

(3) Information relating to any discretionary benefit of a financial nature including the granting of a licence or permit conferred to an individual, including the name of the individual and the exact nature of the benefit is not personal information for the purposes of the Act.

(4) Information about an individual who has been deceased for more than twenty years is not personal information for the purpose of this Act.

Collection of personal information.

30. Personal information may not be collected by or for a public authority unless -

(a) the collection of that information is expressly authorized by or under any written law;

(b) the information is collected for the purposes of law enforcement; or

(c) that information relates directly to and is necessary for an operating programme or activity of the public authority.

Personal information to be collected directly.

31.(1) Where a public authority requires personal information from an individual it shall collect the personal information or cause the personal information to be collected directly from that individual..

(2) Notwithstanding subsection (1), personal information may be collected from a source other than the individual where-

(a) another method of collection is authorized by the individual, by the Commissioner or by any other written law;

(b) the collection of information is necessary for medical treatment of an individual and it is not possible to collect the information directly from that individual or the collection is necessary to obtain authority from that person for another method of collection;

(c) the information is collected for the purpose of –

(i) determining the suitability for an honour or award including an honorary degree, scholarship, prize or bursary;

(ii) proceedings before a court or a judicial or quasi-judicial tribunal;

(iii) collecting a debt or fine or making a payment; or

(iv) law enforcement.

Individual to be informed of purpose.

32.(1) A public authority shall ensure that the individual from whom it collects personal information or causes personal information to be collected is informed of -

(a) the purpose for collecting it;

(b) the legal authority for collecting it; and

(c) the title, business address and business telephone number of an official or employee or the public authority who can answer the individual's questions about the collection.

(2) Subsection (1) shall not apply if compliance with subsection (1) would -

(a) result in the collection of inaccurate information;

(b) defeat the purpose or prejudice the use for which the information is to be collected;

(c) prejudice a law enforcement matter; or

(d) prejudice the defence of Trinidad and Tobago or of any foreign state allied to or associated with Trinidad and Tobago or harm the detection, prevention or suppression of espionage, sabotage or terrorism.

Retention of personal information used for an administrative purpose.

33. Personal information that has been used by a public authority for an administrative purpose shall be retained by the authority for such period of time after it has been used as may be prescribed by Order of the Minister, to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to that information.

Accuracy of personal information.

34. Where the personal information of an individual is in the custody or control of a public authority and the personal information will be used by or on behalf of the public authority to make a decision that directly affects the individual, the public authority shall make every reasonable effort to ensure that the personal information is accurate and complete.

Protection of personal information.

35. A public authority shall protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, alteration, disclosure or disposal.

Storage and access of personal information in Trinidad and Tobago.

36. A public authority shall ensure or take steps to ensure that personal information in its custody or under its control is stored only in Trinidad and Tobago and accessed only in Trinidad and Tobago unless -

(a) the individual to whom the information relates has identified the information and has consented in the prescribed manner to its being stored in or accessed from another jurisdiction; or

(b) the information is stored in or accessed from another jurisdiction that has comparable safeguards as provided by this Act.

Disposal of personal information.

37. A public authority shall dispose of all personal information in its control or custody in accordance with Regulations made by the Minister under this Act.

Use of personal information.

38. Personal information under the custody or control of a public authority shall not, without the consent of the individual to whom it relates, be used by the authority except for the purpose for which the information was obtained or compiled by the public authority, or for a use consistent with that purpose, or for a purpose for which the information may be disclosed by the public authority pursuant to section 42.

Consistent purpose.

39. The use of personal information is consistent with the purposes for which it was obtained or compiled, if the use has a reasonable and direct connection to the purpose, and is necessary for performing the statutory duties of, or for operating a legally authorized programme of a public authority that uses or discloses the information or

causes the information to be used or disclosed.

Limitation on processing of sensitive personal information in possession of public authority.

40.(1) A public authority shall not process sensitive personal information unless it obtains the consent of the person to whom that sensitive personal information relates.

(2) Notwithstanding subsection (1) sensitive personal information may be processed-

(a) by a health care professional for the purposes of health and hospital care where it is necessary for –

(i) preventative medicine and the protection of public health;

(ii) medical diagnosis;

(iii) health care and treatment;

(iv) the management of health and hospital care services;

(b) where it has been made public by the person to whom such information relates;

(c) for research and statistical purposes in accordance with section 43;

(d) in the interest of national security; or

(e) for the purposes of determining access to social services.

Chap. 29:50
Chap. 29:54
Chap. 29:51
Chap. 29:52
Chap. 90:04

(3) For the purpose of this section "health care professional" means a person registered under the –

(a) Medical Board Act;

(b) Dental Profession Act;

(c) Opticians Registration Act;

(d) Pharmacy Board Act; and

(e) Professions Related to Medicine Act.

(4) A person who contravenes this section commits an offence.

Disclosure of personal information in Trinidad and Tobago.

41. Personal information under the custody or control of a public authority shall not be disclosed by the public authority in Trinidad and Tobago without the consent of the individual to whom it relates, except in accordance with sections 42, 43, 44 and 45.

When personal information may be disclosed.

42. Except as provided under any other written law, personal information under the control of a public authority may only be disclosed-

(a) for the purposes for which the information was collected or compiled by the public authority or for a use consistent with that purpose;

(b) for any purpose in accordance with any written law or any order made pursuant to such written law that authorizes such disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

(d) to the Attorney General of Trinidad and Tobago for use in legal proceedings involving the State;

(e) to an investigative body specified by the Minister by Order, on the written request of the investigative body, for the purpose of investigating compliance with any written law or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be provided;

(f) by one law enforcement agency in Trinidad and Tobago to another law enforcement agency within Trinidad and Tobago for the purpose of enforcement of a written law;

(g) to a law enforcement agency in a foreign country under a written agreement, treaty or under the authority of the Government of Trinidad and Tobago;

(h) if the head of the public authority agrees that a compelling circumstance exists that affects the health or safety of any person and if notice of the disclosure is mailed to the last known address of the individual to whom the information relates, unless the head of the public authority has a reasonable belief that providing notification could harm the health or safety of any person;

(i) so that the next of kin or friend of an injured, ill or deceased person may be contacted;

(j) for the purpose of collecting monies owing by an individual to the Government of Trinidad and Tobago or by a public authority to an individual;

(k) for statistical purposes where the disclosure meets the requirements of section 43; or

(l) for archival purposes where the disclosure meets the requirements of section 44.

Disclosure for research and statistical purposes.

43. A public authority may disclose personal information or may cause personal information in its custody or control to be disclosed for a research purpose, including statistical research only if -

(a) the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form;

(b) the information is disclosed on condition that it not be used for the purpose of contacting a person to participate in research;

(c) any record linkage is not harmful to the individual to whom that information is about and the benefits to be derived from the record linkage are clearly in the public interest;

(d) the head of the public authority concerned has approved conditions relating to the following:

(i) security and confidentiality;

(ii) the removal or destruction of the individual identifiers at the earliest reasonable time;

(iii) the prohibition of any subsequent use or

disclosure of that information in individually identifiable form without the express authorization of that public authority; and

(e) the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and any of the public authority's policies and procedures relating to the confidentiality of personal information.

Disclosure for archival or historical purposes.

44. The archives of the Government of Trinidad and Tobago or the archives of a public authority may disclose personal information or cause personal information in its custody or control to be disclosed for archival or historical purposes if-

(a) the disclosure would not be an unreasonable invasion of professional or personal privacy;

(b) the disclosure is for historical research and is in accordance with section 42;

(c) the information concerns someone who has been deceased for twenty or more years; or

(d) the information is in a record that has been in existence for one hundred or more years.

Disclosure of medical information to be restricted.

45. Notwithstanding sections 42, 43 and 44, medical information may not be disclosed by a public authority except-

(a) with the consent of the person to whom such information relates; or

(b) by Order of the court.

Disclosure of personal information outside of Trinidad and Tobago.

46.(1) Where personal information under the custody and control of a public authority is to be disclosed to a party residing in another jurisdiction, the public authority shall inform the individual to whom it relates of the identity of -

(a) the person requesting the information; and

(b) the relevant public authority with responsibility for Data Protection in the other jurisdiction,

and obtain his consent before disclosing the information.

(2) Where a person under subsection (1) does not consent to the release of his personal information, the public authority shall not so disclose.

(3) Subsections (1) and (2) shall not apply where the circumstances set out in section 41exist, but personal information may be limited where the public authority determines that the jurisdiction to which the personal information is being sent does not have comparable standards.

(4) Where a person under subsection (1) consents to the release of his information and the public authority is -

(a) satisfied that the jurisdiction to which the information is being sent has comparable safeguards as provided by this Act, the public authority shall disclose the personal information;

(b) not satisfied that the jurisdiction to which the information is being sent has comparable safeguards the public authority shall refer the matter to the Commissioner for a determination as to whether the other jurisdiction has comparable safeguards as provided by this Act and inform the individual to whom the personal information relates of the referral.

(5) Upon a referral under subsection (2) the Commissioner shall make a determination whether the other jurisdiction has or does not have comparable safeguards as provided by this Act, and inform the public authority accordingly.

(6) Where the public authority is informed that the jurisdiction to which the information is being sent-

(a) has comparable safeguards, the public authority shall inform the person concerned and disclose the personal information;

(b) does not have comparable safeguards, the public authority shall inform the person concerned and obtain his consent for the disclosure-

(i) without limitation; or

(ii) with limitation on the information sharing to the extent necessary to ensure the protection of personal privacy and information.

Privacy impact assessment and mitigation.

47.(1) Every Ministry shall prepare a privacy impact assessment, in the form prescribed by the Minister, for any proposed enactment, system, project, programme or activity.

(2)Upon preparation of a privacy impact assessment, every Ministry shall submit such privacy impact assessment to the Commissioner for approval.

(3)Where a privacy impact assessment has been submitted in accordance with subsection (2) the Commissioner shall evaluate such privacy impact assessment in accordance with the General Privacy Principles set out in section 6 and where necessary, make recommendations to the Ministry for amendments.

(4) Where the Commissioner makes a recommendation under subsection (3), the Ministry shall make the necessary amendments to its privacy impact assessment.

(5) Every Ministry shall take all reasonable steps in accordance with its privacy impact assessment to avoid unnecessary intrusions into personal privacy when designing, implementing or enforcing enactments, systems, projects, programmes or activities.

Personal information banks.

48.(1) The head of a public authority shall cause to be included in personal information banks, all personal information under the control or in the custody of the public authority that-

(a) has been used, is being used or is available for the use for an administrative purpose; or

(b) is organized or intended to be retrieved by means of the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

(2) Notwithstanding subsection (1), personal information under the custody or control of the Archives of Government of Trinidad and Tobago that has been transferred to it by a public authority for historical or archival purposes shall not be included in personal information banks.

Information sharing.

49. Where a public authority intends to share information with other public authorities, it shall do so only pursuant to an agreement in a manner prescribed by the Commissioner by Order.

Data matching shall be approved by Commissioner.

50.(1) Subject to subsection (5), before a public authority matches personal information from a set of data with personal information from another set of data, whether or not pursuant to an information sharing agreement, the public authority shall obtain the written authorization of the Commissioner.

(2) In determining whether to authorize data matching by a public authority or public authorities, the Commissioner shall consider whether or not -

(a) the objective of the matching programme relates to a matter of significant public importance;

(b) the matching programme would achieve the objective in a way which would achieve monetary savings that are both significant and quantifiable or will achieve other significant benefits to society;

(c) the public interest in allowing the matching programme to proceed outweighs the public interest in adhering to the General Privacy Principles set out in section 6 that the programme would otherwise contravene; or

(d) the programme involves information matching on a scale that is excessive, having regard to the number of public authorities that will be involved in the programme and the amount of details about the individual that would be matched under the programme.

(3) The Data Commissioner shall complete his

determination in respect of the data matching request within sixty days of the request.

(4) In approving data matching by a public authority or public authorities, the Commissioner may impose whatever terms and conditions that he considers appropriate.

(5) Where the Data Commissioner fails to complete his determination in respect of a data matching request under subsection (3), the public authority may apply to the Minister for a determination of the matter.

(6) In giving his authorization under subsection (1), the Data Commissioner may give covering authorization to allow the matching of data where such matching is part of a system of practice approved by him.

Personal information index.

51. The Minister shall publish periodically, but not less than annually, an index of the personal information that is held by the public authorities that includes a summary of the following:

(a) the personal information banks that are in the custody or control of each public authority;

(b) the information sharing agreements entered into by any public authority with another public authority or other person;

(c) the data matching activities approved by the Commissioner;

(d) the contact information of the official to whom requests relating to personal information contained in the data bank should be sent;

(e) a statement of the purposes for which personal information in the data bank was obtained or compiled and a statement of the uses consistent with those purposes for which the information is used or disclosed;

(f) a statement of the retention and disposal standards and practices that apply to the personal information in the data bank; and

(g) privacy impact assessments prepared by any Ministry of the Government of Trinidad and Tobago.

Right of access to personal information.

52.(1) Subject to section 53 every individual who is a citizen of or resident in Trinidad and Tobago has a right to and shall on request, be given access to-

(a) personal information about that individual contained in a personal information bank in the custody and control of a public authority;

(b) any other personal information about the individual under the custody or control of a public authority with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the public authority.

(2) A request for access to personal information shall be made to the public authority that has control of the personal information bank or of the information, as the case may be, in the form approved by the Commissioner.

(3) The head of a public authority may, where reasonable and in appropriate circumstances, provide personal information in accordance with the provisions of this Act in response to an oral request.

Chap. 18:01

(4) For the purpose of this section "resident" has the meaning assigned to it by the Immigration Act.

Refusal of access to personal information.

53.(1) A head of a public authority may refuse to disclose personal information to the individual to whom the information relates where-

(a) the disclosure would constitute an unjustified invasion of another individual's personal privacy;

(b) it is a correctional record where the disclosure could reasonably be expected to reveal information supplied in confidence;

(c) it is evaluative or opinion material compiled solely for the purpose of determining suitability,

eligibility or qualifications for employment or for the awarding of government contracts and other benefits where the disclosure would reveal the identity of a source who furnished information to the institution in circumstances where it may reasonably be assumed that the identity of the source would be held in confidence;

Chap. 22:02

(d) a disclosure would result in disclosure of information that is exempt from disclosure under Part IV of the Freedom of Information Act.

(2) The head of a public authority may disregard requests from an individual for access to that individual's personal information where it would unreasonably interfere with the operations of the public authority because of the repetitious or systematic nature of the requests or the requests are frivolous or vexatious.

Severance and refusal to disclose existence of information.

54.(1) A head of a public authority shall make every effort to sever information that is exempt from disclosure pursuant to section 53 from information that may be made available to the individual requesting access to his personal information and make the non-exempt information available.

(2) Where acknowledgment of the existence of information that is exempt from disclosure would reveal critical information about the nature of contents of the information, the head of the public authority may refuse to disclose the existence of the information.

Exercise of rights of deceased persons etc.

55. Any right or power conferred on an individual by this Act may be exercised-

(a) where the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the individual's estate;

(b) by the individual's attorney under a power of attorney;

(c) the individual's guardian; or

(d) where the individual is less than eighteen years of age, by a person who has lawful custody of the individual.

Responsibilities of public authorities.

56.(1) Where a request is made for access to personal information pursuant to section 52, the head of the public authority shall, within thirty days after the request is received where access is-

(a) granted in whole or in part, give the information to the individual who made the request; or

(b) refused in whole or in part, give the individual who made the request a written response stating-

(i) that the information does not exist; or

(ii) the specific provision of the Act on which a refusal could reasonably be expected to be based if the information existed;

(c) refused in whole or in part, give the individual who made the request information regarding the right of appeal to the Commissioner.

(2) Where access is granted in whole or in part, the head of the public authority shall ensure that the information is available in a comprehensive form, including where reasonable, comprehensible to an individual with a sensory disability.

Right to request correction of personal information.

57.(1) Where an individual believes there is an error or omission in his personal information, the individual may request the head of the public authority that has the information in its custody or under its control, to correct the information.

(2) If no correction is made in response to a request under subsection (1), the head of the public authority shall annotate the information with the correction that was requested but not made and notify the individual who made the request that no correction was made.

(3) On correcting or annotating personal information under this section, the head of a public authority shall notify any other public authority or any third party to whom that information has been disclosed

during the one-year period before the correction was requested, of such correction or annotation.

(4) Upon being notified under subsection (3) of a correction or annotation of personal information, a public authority shall make the correction or annotation on any record of that information in its custody or control.

Appeal to Data Commissioner.

58. An individual who has filed a request for his personal information pursuant to section 52 or who has requested correction of personal information pursuant to section 57 may appeal any decision of the head of the public authority to the Data Commissioner.

Time for application.

59. An appeal to the Commissioner under section 58 shall be made within six weeks of the date when the notice was given of the decision appealed from, by filing with the Commissioner written notice of appeal.

Immediate dismissal.

60. The Commissioner may dismiss an appeal if the notice of appeal does not present a reasonable basis for concluding that the personal information to which the notice relates exists.

Informing of notice of appeal.

61. Upon receiving the notice of appeal, the Commissioner shall inform the head of the public authority concerned and any other affected person of the notice of appeal.

Mediation.

62. The Commissioner may authorize a mediator to investigate the circumstances of the appeal and to try to effect a settlement of the matter under appeal.

Enquiry by the Commissioner.

63.(1) The Commissioner may conduct an enquiry to review the decision of the head of a public authority if the Commissioner has-

(a) not authorized a mediator to conduct an investigation under section 62; or

(b) authorized a mediator to conduct an investigation under section 62, but no settlement has been reached.

(2) Where the Commissioner conducts an enquiry under this section he may on the conclusion of such enquiry either-

(a) affirm the decision of the head of the public Authority; or

(b) order the head of the public authority to release the personal information or make the corrections requested.

Enquiry in private.

64. The enquiry by the Commissioner or a mediator and any meetings held by a mediator with parties to the appeal may be conducted in private.

Representations.

65. The individual who requested access to personal information, the head of the public authority concerned and any affected party shall be given the opportunity to make representations to the Commissioner, but none is entitled to-

(a) be present during;

(b) have access to; or

(c) comment on,

representations made to the Commissioner by any other person.

Right to counsel or an agent.

66. An individual who requests access to personal information, the head of the public authority concerned and any affected party may be represented by counsel or an agent.

Burden of proof.

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

PART IV

PROTECTION OF PERSONAL DATA BY THE PRIVATE SECTOR

Application of General Privacy Principles.

68. A person who-

(a) collects, retains, manages, uses, processes or stores personal information in Trinidad and Tobago;

(b) collects personal information from individuals in Trinidad and Tobago; or

(c) uses an intermediary or telecommunications service provider located in Trinidad and Tobago to provide a service in furtherance of paragraph (a) or (b),

shall follow the General Privacy Principles set out in section 6 in dealing with personal information.

Codes of practice.

69. The Commissioner shall consult with industry to promote the application of the General Privacy Principles through the development of codes of practice through such means as-

(a) providing guidance on the development of codes of practice;

(b) providing guidance on compliant resolution mechanisms;

(c) fostering education on the General Privacy Principles;

(d) working with government and private sector bodies to promote awareness of codes of conduct among consumers; and

(e) taking any action that appears to the Commissioner to be appropriate.

Commissioner may require development of code of conduct.

70.(1) Notwithstanding section 68 where, in the opinion of the Commissioner, the public interest warrants the immediate and mandatory development of codes of conduct dealing with the application of the General Privacy Principles to a particular industry, economic sector, or

activity, the Commissioner may, by Order, require the development of a code of conduct and set a time limit for its development.

(2) Subject to subsection (1) where there is an appropriate government regulator of an industry, economic sector or activity, the Commissioner may request the regulator to oversee the development of the code of conduct for that industry, economic sector or activity.

Cross border disclosure of personal information.

71.(1) Where a mandatory code of conduct is developed pursuant to section 70, it shall require at a minimum that personal information under the custody or control of an organization shall not be disclosed by that organization to any third party without the consent of the individual to whom it relates, except in general, where such information is disclosed for the purposes-

(a) for which the information was collected or for use consistent with that purpose;

(b) of a Court Order; or

(c) of complying with any written law.

(2) Where personal information under the custody and control of an organization is to be disclosed to a party residing in another jurisdiction, the organization shall inform the individual to whom it relates of the identity of -

(a) the person requesting the information; and

(b) the relevant public authority with responsibility for Data Protection in the other jurisdiction,

and obtain his consent before disclosing the information.

(3) Where a person under subsection (2) does not consent to the release of his personal information the organization shall not so disclose.

(4) Where a person under subsection (2) consents to the disclosure of his information and the organization is -

(a) satisfied that the jurisdiction to which the information is being sent has comparable safeguards as provided by this Act, the organization shall disclose the personal information;

(b) not satisfied that the jurisdiction to which the information is being sent has comparable safeguards the organization shall refer the matter to the Commissioner for a determination as to whether the other jurisdiction has comparable safeguards as provided by this Act and inform the individual to whom the personal information relates of the referral.

(5) Upon a referral under subsection (4) the Commissioner shall make a determination whether the other jurisdiction has or does not have comparable safeguards as provided by this Act, and inform the organization accordingly.

(6) Where the organization is informed that the jurisdiction to which the information is being sent-

(a) has comparable safeguards, the organization shall inform the person concerned and disclose the personal information;

(b) does not have comparable safeguards, the organization shall inform the person concerned and obtain his consent for the disclosure-

(i) without limitation on the personal information; or

(ii) with limitation on the personal information sharing to the extent necessary to ensure the protection of personal privacy and information.

Approval of code of conduct.

72.(1) Where a mandatory code of conduct is developed the sector shall apply to the Commissioner for the approval of such code prior to its use.

(2) Where a voluntary code of conduct is developed the sector may apply to the Commissioner for the approval of such code prior to its use

(3) The Commissioner may approve a code of conduct dealing with compliance with the General Privacy Principles set out in section 6 developed by an industry sector, an industry organization or a professional body.

(4) Where the Commissioner is satisfied that a code of conduct submitted for approval in accordance with subsection (1) or (2) meets the requirements set out in subsection (5), he shall approve the code of conduct.

(5) In approving a code of conduct, the Commissioner shall consider-

(a) compliance with the General Privacy Principles set out in section 6;

(b) use and adequacy of dispute resolution mechanisms within the industry as well as within individual firms;

(c) the potential for development or encouragement of anti-competitive conduct;

(d) the adequacy of the process used to develop the code of conduct, including involvement of stakeholders, such as relevant consumers, suppliers and other interested groups;

(e) the role of industry sector regulators if any; and

(f) any other matters that the Commissioner considers relevant.

Mandatory codes of conduct.

73.(1) Where the Commissioner has approved a code of conduct, the Minister may by Order make compliance with the code mandatory with respect to those to whom the code of conduct applies under this Act.

(2) An Order made by the Minister under subsection (1), shall be subject to negative resolution of Parliament.

(3) Where a code of conduct has been made mandatory

under subsection (1), the persons or enterprises to whom or to which it applies shall comply with the provisions of the code of conduct.

(4) Without limiting the generality of subsection (1), where a government regulator has jurisdiction over an industry, economic sector or activity so that the code of conduct dealing with the application of the General Privacy Principles can be made mandatory pursuant to other legislation, the regulator may make a code of conduct approved by the Commissioner mandatory.

(5) Where an industry regulator has mandated compliance in dealing with the protection of personal privacy that has been approved by the Commissioner and the legislation under which the code of conduct has been made mandatory has adequate provisions for complaint resolution and sanctions for non-compliance with the provisions of the code of conduct, the Commissioner may forebear from exercising his powers with respect to compliance.

Limitation on processing of sensitive information in the possession of a corporation.

74.(1) A corporation shall not process sensitive personal information in its possession unless it obtains the consent of the person to whom that sensitive personal information relates.

(2) Notwithstanding subsection (1), sensitive personal information may be processed-

(a) by a health care professional for the purposes of health and hospital care where it is necessary for –

(i) preventative medicine and the protection of public health;

(ii) medical diagnosis;

(iii) health care and treatment;

(iv) the management of health and hospital care services.

(b) where it has been made public by the person to whom such information relates;

(c) for research and statistical purposes in accordance with section 43;

(d) where the disclosure is required by written law.

(3) For the purpose of this section "health care professional" means a person registered under the –

Chap. 29:50
Chap. 29:54
Chap. 29:51
Chap. 29:52
Chap. 90:04

(a) Medical Board Act;

(b) Dental Profession Act;

(c) Opticians Registration Act;

(d) Pharmacy Board Act; and

(e) Professions Related to Medicine Act.

(4) A person who contravenes this section commits an offence.

Refusal of request for access to personal information.

75.(1) The head of an organization subject to a mandatory code of conduct, may upon the authorization of the Commissioner disregard a request from an individual for access to that individual's personal information where it would unreasonably interfere with the operations of the organization because of the repetitious or systematic nature of the requests or the requests are frivolous or vexatious.

(2) Where an organization disregards a request under subsection (1) it shall notify the individual making request.

Request for review or complaint to the Commissioner.

76. Where an organization is subject to a mandatory code of conduct and an individual has a reasonable belief that the organization has within its custody or control personal information regarding that individual, the individual may-

(a) where the individual has requested access to or the correction of personal information, held by an organisation and the organisation has refused such request, ask the Commissioner to conduct a review of the resulting decision, act or failure to act of the organization; or

(b) make a complaint to the Commissioner regarding an alleged failure of the organization to comply with the provisions of the mandatory code of conduct.

Time for application for review or complaint.

77. A request for a review by or a complaint to the Commissioner shall be made within six weeks of the date of the decision or six weeks from which the failure to comply with the mandatory codes of conduct first became known or should have become known.

Immediate dismissal of request for review or complaint.

78. The Commissioner may not entertain-

(a) a request for a review of the decision where the written request does not present a reasonable basis for concluding that the personal information, to which the request relates, exists; or

(b) a complaint under section 75 where the written complaint does not contain enough particulars to make a determination of non-compliance with the mandatory code of conduct on the part of the organization.

Notification of request or complaint.

79. Upon receiving the written request or complaint under section 75, the Commissioner shall inform the head of the organization concerned and any other affected person of the request or complaint.

Enquiry of request or complaint.

80.(1) Subject to section 81(2), the Commissioner may conduct an enquiry into a request or complaint under section 76.

(2) Where the Commissioner conducts an enquiry under this section he may, on the conclusion of such enquiry either-

(a) affirm the decision of the organization; or

(b) order the head of an organization to release the personal information requested.

Mediation of request.

81.(1) The Commissioner may authorize a mediator to investigate the circumstances of the request and to try to effect a settlement of the matter.

(2) Where the Commissioner has-

(a) not authorized a mediator to conduct an investigation under subsection (1); or

(b) authorized a mediator to conduct an investigation under subsection (1) but no settlement has been reached,

he may conduct an enquiry into a request under section 80.

Enquiry of request to be conducted in private.

82. An enquiry by the Commissioner or a mediator and any meetings held by a mediator with parties to the request may be conducted in private.

Representations.

83. An individual who requested access to personal information, the head of the organization concerned and any affected party shall be given the opportunity to make representations to the Commissioner, but none is entitled to-

(a) be present during;

(b) have access to; or

(c) comment on,

representations made to the Commissioner by any other person.

Duties of directors.

84. Every director and officer of a corporation shall take reasonable care to ensure that the corporation complies with-

(a) this Act and the regulations made thereunder; and

(b) any Orders imposed by the Commissioner or his delegate.

PART V

CONTRAVENTION AND ENFORCEMENT

Obstruction.

85 A person who wilfully obstructs the Data Commissioner or any other person acting for or under the direction of the Commissioner in the course of carrying out an audit or an investigation, commits an offence.

False and misleading statements.

86.(1) A person who makes a request for access to or correction of personal information under false pretences, commits an offence.

(2) A person who wilfully makes a false statement to mislead or attempts to mislead the Commissioner in the performance of his functions under this Act, commits an offence.

Failure to comply with an order.

87. A person who fails to comply with an order of the Commissioner, commits an offence.

Violation of whistle-blowing provisions.

88. A person who contravenes the provisions of section 98, commits an offence.

Offence for not complying with mandatory code.

89. Where a person to whom a mandatory code of conduct applies under section 73 fails to comply with such mandatory code of conduct, he commits an offence.

Contravention of Act.

90.(1) A person who wilfully discloses personal information in contravention of this Act, commits an offence.

(2) A person who wilfully maintains a personal information bank that contravenes this Act, commits an offence.

Breach of obligations of confidentiality.

91. A person who breaches the confidentiality obligations established by section 25, commits an offence.

Offences by directors and officers.

92. Where a corporation commits an offence under this Act, any officer, director or agent of the corporation who directed, authorized, assented to, acquiesced in or participated in the commission of the offence is a party to and commits an offence and is liable to the punishment provided for the offence, whether or not the corporation has been prosecuted and convicted.

Penalties.

93.(1) A person who commits an offence under this Act is liable upon-

(a) summary conviction to a fine of not more than fifty thousand dollars or to imprisonment for a term of three years;

(b) conviction on indictment to a fine of not more than one hundred thousand dollars or to imprisonment for a term of not more than five years.

(2) Where the offence under this Act is committed by a body corporate, the body corporate shall be liable upon-

(a) on summary conviction to a fine of two hundred and fifty thousand dollars; and

(b) conviction of indictment to a fine of five hundred thousand dollars.

Penalties for corporations.

94.(1) Where a corporation contravenes any of the provisions of this Act, the Court may impose a fine up to ten per cent of the annual turnover of the enterprise.

(2) In imposing a fine under subsection (1) the Court shall take into account-

(a) the estimate of the economic cost of the contravention to the consumers, users of the services in question or any other person affected by the contravention;
(b) the estimate of the economic benefit of the contravention to the enterprise;
(c) the time for which the contravention is in effect if continuing;
(d) the number and seriousness of any other contraventions, if any, committed by the corporation; and
(e) any other matter the Court may consider appropriate in the circumstances.

PART VI

MISCELLANEOUS

Costs of audit.

95. The Minister may order a public authority or a corporation to pay the costs reasonably incurred in the performance of an audit pursuant to sections 20 and 21.

Jurisdiction of the Court.

96.(1) The Court shall have jurisdiction to hear and determine -

(a) applications by the Data Commissioner for any Order which the Court considers appropriate to facilitate the enforcement of any provisions of this Act;

(b) upon application by the Data Commissioner cases involving any contravention of the provisions of this Act and make such appropriate Orders in relation thereto.

Whistle-blowing protection.

97. An employer whether or not a public authority, shall not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee or deny that employee a benefit, because -

(a) the employee acting in good faith, and on the basis of reasonable belief has-

(i) notified the Commissioner that the employer or any other person has contravened or is about to contravene this Act;

(ii) done or stated the intention of doing anything that is required to be done in order to avoid having any person contravene this Act;

(iii) refused to do or stated the intention of refusing to do anything that is in contravention of this Act; or

(b) the employer believes that the employee will do anything described in paragraph (a).

Regulations.

98.(1) The Minister may make Regulations for the purpose of-

(a) prescribing anything required to be prescribed under this Act; and

(b) giving effect to the provisions of this Act.

(2) Regulations made under this section shall be subject to negative resolution of Parliament.

Chap. 22:20 amended.

99. The Freedom of Information Act is amended in-

(a) section 4 -

(i) by inserting after the definition of "applicant" the following definitions:

"Data Commissioner" means the person appointed pursuant to section 8 of the Data Protection Act;

"decision of a public authority" means the refusal of a public authority to grant access to an official document or the failure of a public authority to comply with sections 15 or 16(1) herein;";

(ii) by deleting the definition of "personal information" and substituting the following definition:

"personal information" has the meaning assigned to it in the Data Protection Act;";

(iii) in the definition of "public authority" -

(A) in paragraph (j), by deleting the word "or";

(B) by inserting after the word "control;" the word "or";

(C) by inserting after paragraph (k) the following new paragraph:

"(l) the Data Commissioner as appointed under section 8 of the Data Protection Act.";

(b) in section 30 by deleting subsections (1), (2) and (3) and substituting the following subsections:

"(1) A document is an exempt document if its disclosure under this Act would involve the disclosure of personal information in a manner inconsistent with the Data Protection Act.

(2) The provisions of subsection (1) shall not apply to a request by an individual for his own personal information, which requests shall be treated as a request under the Data Protection Act.

(3) Where a request by a person other than a person referred to in subsection (2) is made to a public authority for access to a document containing personal information, the public authority shall proceed in accordance with the Data Protection Act in deciding whether to grant access to such request.";

(c) in section 36 by deleting subsection (1) and substituting the following subsection:

"(1) Where a document (whether or not it is one to which access has been given under this Act) contains personal information of an individual and that individual believes that the information is inaccurate, he shall proceed, and the public authority shall address the matter, in accordance with section 58 of the Data Protection Act.";

(d) in section 38A -

(i) in subsection (1) by deleting the word "Ombudsman" wherever it occurs and substituting the word "Data Commissioner";

(ii) in subsection (2) by deleting the word "Ombudsman" and substituting the word "Data Commissioner"; and

(iii) by deleting subsection (3); and

(e) in section 39 by deleting subsection (3).

SCHEDULE

(Section 8)

FORM OF OATH (AFFIRMATION) FOR DATA COMMISSIONER

I, A. B. having been appointed Data Commissioner do swear by …… (solemnly affirm) that I bear true faith and allegiance to Trinidad and Tobago and will uphold the Constitution and the law, that I will conscientiously, impartially and to the best of my knowledge, judgement and ability discharge the functions of my office and do right to all manner of people after the laws and usages of Trinidad and Tobago without fear or favour, affection or ill-will

Passed in the House of Representatives this day of , 2008

Clerk of the House

I confirm the above.

Speaker

Passed in the Senate this day of , 2008

Clerk of the Senate

I confirm the above.

President.