A BILL

entitled

PERSONAL INFORMATION PROTECTION ACT 2016

TABLE OF CONTENTS

WHEREAS it is expedient to regulate the use of personal information by organisations in a manner which recognises both the need to protect the rights of individuals in relation to their personal information and the need for organisations to use personal information for legitimate purposes;

Be it enacted by The Queen's Most Excellent Majesty, by and with the advice and consent of the Senate and the House of Assembly of Bermuda, and by the authority of the same, as follows:

PART 1

INTERPRETATION AND SCOPE

Citation

1 This Act may be cited as the Personal Information Protection Act 2016.

Interpretation

2 In this Act, unless the context otherwise requires—

"applicant" means an individual who makes a written request in accordance with section 20;

"binding corporate rules" means personal information protection policies approved by the Commissioner which are adhered to by an organisation for transfers or sets of transfers of personal information;

"biometric information" means any information relating to the physical, physiological or behavioural characteristics of an individual which allows his unique identification, such as facial images or fingerprint information;

"business contact information" means an individual's name, position name or title, business telephone number, business address, business e-mail, business fax number and other similar business information;

"Commissioner" means the Privacy Commissioner appointed under section 26;

"genetic information" means all personal information relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual resulting, in particular, from an analysis of a biological sample from the individual in question;

"individual" means a natural person;

"minimum requirements" means the requirements of sections 5, 8,11,12, and 13;

"Minister" means the Minister to whom responsibility for this Act has been assigned;

"organisation" means any individual, entity or public authority that uses personal information;

"overseas third party" means an individual or organisation not domiciled in Bermuda;

"personal information" means any information about an identified or identifiable individual;

"prescribe" means prescribe by regulations made under section 48;

"publicly available information" means personal information about an individual which the individual knowingly makes or permits to be made available to the public, or which is legally obtained or accessed from—

(a) government records that are available to the public; or

(b) information required by law to be made available to the public;

"sensitive personal information" has the meaning given in section 7(1);

"use" or "using", in relation to personal information, means carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating or otherwise making available, combining, blocking, erasing or destroying it.

Application

3 Except as provided by this Act, this Act applies to every organisation that uses personal information in Bermuda where that personal information is used wholly or partly by automated means and to the use other than by automated means of personal information which form, or are intended to form, part of a structured filing system.

Exclusions

4 (1) This Act does not apply to—

(a) the use of personal information for personal or domestic purposes;

(b) the use of personal information for artistic, literary or journalistic purposes with a view to publication in the public interest in so far as is necessary to protect the right to freedom of expression;

(c) the use of business contact information for the purpose of contacting an individual in his capacity as an employee or official of an organisation;

(d) personal information about an individual who has been dead for at least 20 years;

(e) personal information about an individual that has been in existence for at least 150 years;

(f) personal information transferred to an archival institution where access to the personal information was unrestricted or governed by an agreement between the archival institution and the donor of the personal information before the coming into operation of this Act;

(g) personal information contained in a court file and used by a judge of any court in Bermuda or used as part of judicial administration or relating to support services provided to the judges of any court in Bermuda, but only where such personal information is necessary for judicial purposes;

(h) personal information contained in a personal note, communication or draft decision created by or for an individual who is acting in a judicial, quasi-judicial or adjudicative capacity;

(i) personal information used by a member of the House of Assembly or the Senate where such use relates to the exercise of his political function and the personal information is covered by parliamentary privilege.

(2) If an organisation has under its control personal information about an individual that was acquired before the coming into force of this Act, that personal information, for the purposes of this Act—

(a) is deemed to have been collected pursuant to consent given by that individual; and

(b) may be used by the organisation for the purposes for which the information was collected.

(3) This Act shall not apply so as to—

(a) affect any legal privilege;

(b) limit the information available by law to a party to any legal proceedings; or

(c) limit or affect the use of information that is the subject of trust conditions or undertakings to which a lawyer is subject.

(4) If a provision of this Act is inconsistent or in conflict with a provision of another enactment, the provision of this Act prevails unless this Act is inconsistent with or in conflict with a provision in the Human Rights Act 1981, in which case, the Human Rights Act 1981 prevails.

(5) This Act applies notwithstanding any agreement to the contrary, and any waiver or release given of the rights, benefits or protections provided under this Act is against public policy and void.

PART 2

GENERAL PRINCIPLES AND RULES

Responsibility and compliance

5 (1) Every organisation shall adopt suitable measures and policies to give effect to its obligations and to the rights of individuals set out in this Act.

(2) The measures and policies in subsection (1) shall be designed take into account the nature, scope, context and purposes of the use of personal information and the risk to individuals by the use of the personal information.

(3) Where an organisation engages (by contract or otherwise) the services of a third party in connection with the use of personal information, the organisation remains responsible for ensuring compliance with this Act at all times.

(4) An organisation shall designate a representative ("privacy officer") for the purposes of compliance with this Act who will have primary responsibility for communicating with the Commissioner.

(5) A group of organisations under common ownership or control, may appoint a single privacy officer provided that a privacy officer is accessible from each organisation.

(6) A privacy officer designated under subsection (4) may delegate his duties to one or more individuals.

(7) In meeting its responsibilities under this Act, an organisation shall act in a reasonable manner.

Conditions for using personal information

6 (1) Subject to subsections (2), (3) and (4), an organisation may use an individual's personal information only if one or more of the following conditions are met—

(a) the personal information is used with the consent of the individual where the organisation can reasonably demonstrate that the individual has knowingly consented;

(b) except in relation to sensitive personal information, a reasonable person giving due weight to the sensitivity of the personal information would consider—

(i) that the individual would not reasonably be expected to request that the use of his personal information should not begin or cease; and

(ii) that the use does not prejudice the rights of the individual;

(c) the use of the personal information is necessary—

(i) for the performance of a contract to which the individual is a party; or

(ii) for the taking of steps at the request of the individual with a view to entering into a contract;

(d) the use of the personal information is pursuant to a provision of law that authorises or requires such use;

(e) the personal information is publicly available information and will be used for a purpose that is consistent with the purpose of its public availability;

(f) the use of the personal information is necessary to respond to an emergency that threatens the life, health or security of an individual or the public;

(g) the use of the personal information is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the organisation or in a third party to whom the personal information is disclosed; or

(h) the use of the personal information is necessary in the context of an individual's present, past or potential employment relationship with the organisation.

(2) For the purpose of relying on consent as a condition for the use of personal information under subsection (1)(a)—

(a) an organisation shall provide clear, prominent, easily understandable, accessible mechanisms for an individual to give consent in relation to the use of his personal information;

(b) an organisation is not obliged to provide such mechanisms where it can be reasonably implied from the conduct of an individual that he consents to the use of his personal information for all intended purposes that have been notified to him, but this does not apply to sensitive personal information;

(c) when an individual consents to the disclosure of his personal information by an intermediary for a specified purpose, that individual will be deemed to have consented to the use of that personal information by the receiving organisation for the specified purpose;

(d) an individual will be deemed to have consented to the use of his personal information for the purpose of coverage or enrolment under an insurance, trust, benefit or similar plan if the individual has an interest in or derives a benefit from that plan.

(3) If an organisation is unable to meet any of the conditions of subsection (1), then it may use personal information only if—

(a) the personal information was collected from, or is disclosed to, a public authority which is authorised or required by a statutory provision to provide the personal information to, or collect it from, the organisation;

(b) the use of the personal information is for the purpose of complying with an order made by a court, individual or body having jurisdiction over the organisation;

(c) the use of the personal information is for the purpose of contacting the next of kin or a friend of an injured, ill or deceased individual;

(d) the use of the personal information is necessary in order to collect a debt owed to the organisation or for the organisation to repay to the individual money owed by the organisation;

(e) the use of the personal information is in connection with disclosure to the surviving spouse or a relative of a deceased individual if, in the reasonable opinion of the organisation, the disclosure is appropriate; or

(f) the use of the personal information is reasonable to protect or defend the organisation in any legal proceeding.

(4) Where an organisation transfers personal information to an overseas third party, in addition to complying with the obligations of subsections (1) to (3), the organisation must also meet the obligations under section 15.

Sensitive personal information

7 (1) "Sensitive personal information" means any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information.

(2) No organisation shall, without lawful authority, use sensitive personal information identified in subsection (1) in order to discriminate against any person contrary to any provision of Part II of the Human Rights Act 1981.

(3) For the purposes of subsection (2), sensitive personal information is used with lawful authority if and only to the extent that it is used—

(a) with the consent of any individual to whom the information relates;

(b) in accordance with an order made by either the court or the Commissioner;

(c) for the purpose of any criminal or civil proceedings; or

(d) in the context of recruitment or employment where the nature of the role justifies such use.

(4) The Minister may make an order, subject to the negative resolution procedure, to amend the definition of "sensitive personal information" in subsection (1).

Fairness

8 An organisation shall use personal information in a lawful and fair manner.

Privacy notices

9 (1) An organisation shall provide individuals with a clear and easily accessible statement ("privacy notice") about its practices and policies with respect to personal information, including—

(a) the fact that personal information is being used;

(b) the purposes for which personal information is or might be used;

(c) the identity and types of individuals or organisations to whom personal information might be disclosed;

(d) the identity and location of the organisation, including information on how to contact it about its handling of personal information;

(e) the name of the privacy officer;

(f) the choices and means the organisation provides to a individuals for limiting the use of, and for accessing, rectifying, blocking, erasing and destroying, his personal information.

(2) Organisations shall take all reasonably practicable steps to ensure that the privacy notice is provided either before or at the time of collection of personal information, or, where that is not possible, as soon thereafter as is reasonably practicable.

(3) Organisations are not obliged to provide a privacy notice if—

(a) all of the personal information held by it is publicly available information; or

(b) the organisation can reasonably determine that all uses made, or to be made, of the personal information are within the reasonable expectations of the individual to whom the personal information relates.

Purpose limitation

10 (1) An organisation shall use personal information only for the specific purposes under section 9(1)(b) or for purposes that are related to those specific purposes.

(2) Subsection (1) shall not apply—

(a) when the use of the personal information is with the consent of the individual whose personal information is used;

(b) when the use of the personal information is necessary to provide a service or product required by the individual;

(c) where the use of personal information is required by any rule of law or by the order of the court;

(d) where the use of the personal information is for the purpose of detecting or monitoring fraud or fraudulent misuse of personal information; or

(e) where the personal information is used for the purposes of scientific, statistical or historical research subject to the appropriate safeguards for the rights of the individual.

Proportionality

11 An organisation shall ensure that personal information is adequate, relevant and not excessive in relation to the purposes for which it is used.

Integrity of personal information

12 (1) An organisation shall ensure that any personal information used is accurate and kept up to date to the extent necessary for the purposes of use.

(2) An organisation shall ensure that personal information for any use is not kept for longer than is necessary for that use.

Security safeguards

13 (1) An organisation shall protect personal information that it holds with appropriate safeguards against risk, including—

(a) loss;

(b) unauthorised access, destruction, use, modification or disclosure; or

(c) any other misuse.

(2) Such safeguards shall be proportional to—

(a) the likelihood and severity of the harm threatened by the loss, access or misuse of the personal information;

(b) the sensitivity of the personal information (including in particular whether it is sensitive personal information); and

(c) the context in which it is held,

and shall be subject to periodic review and reassessment.

Breach of security

14 (1) In case of a breach of security leading to the loss or unlawful destruction or unauthorised disclosure of or access to personal information which is likely to adversely affect an individual, the organisation responsible for that personal information shall, without undue delay—

(a) notify the Commissioner of the breach; and

(b) then notify any individual affected by the breach.

(2) The notification to the Commissioner under subsection (1) shall describe—

(a) the nature of the breach;

(b) its likely consequences for that individual; and

(c) the measures taken and to be taken by the organisation to address the breach,

so that the Commissioner can determine whether to order the organisation to take further steps and for the Commissioner to maintain a record of the breach and the measures taken.

Transfer of personal information to an overseas third party

15 (1) When an organisation transfers to an overseas third party personal information for use by that overseas third party on behalf of the organisation, or for the overseas third party's own business purposes, the organisation remains responsible for compliance with this Act in relation to that personal information.

(2) Before making any such transfer, the organisation shall assess the level of protection provided by the overseas third party for that personal information.

(3) When assessing the level of protection in subsection (2), an organisation shall consider the level of protection afforded by the law applicable to such overseas third party and the Minister, on the recommendation of the Commissioner, may designate any jurisdiction as providing a comparable level of protection for the purposes of this section.

(4) If the organisation reasonably believes that the protection provided by the overseas third party is comparable to the level of protection required by this Act, which may be evidenced by the third party's adoption of a certification mechanism recognised by the Commissioner, the organisation may rely on such comparable level of protection while the personal information is being used by the overseas third party.

(5) Where subsection (4) is not satisfied, the organisation shall employ contractual mechanisms, corporate codes of conduct including binding corporate rules, or other means to ensure that the overseas third party provides a comparable level of protection.

(6) Notwithstanding subsections (1) to (5), an organisation may transfer personal information to an overseas third party for use by that overseas third party on behalf of the organisation or for the overseas third party's own business purposes, if—.

(a) the transfer of the personal information is necessary for the establishment, exercise or defence of legal rights; or

(b) the organisation assesses all the circumstances surrounding the transfer of personal information to the overseas third party and reasonably considers the transfer of personal information is—

(i) small-scale;

(ii) occasional; and

(iii) unlikely to prejudice the rights of an individual.

Personal information about children in the information society

16 (1) Where an organisation uses personal information about a child in the provision of an information society service and—

(a) the service is targeted at children; or

(b) the organisation has actual knowledge that it is using personal information about children,

and consent is relied upon, subject to subsection (2) the organisation must obtain consent from a parent or guardian before the personal information is collected or otherwise used.

(2) An organisation—

(a) shall be reasonably satisfied that consent obtained under subsection (1) is verifiable so that it can be obtained only from the child's parent or guardian; and

(b) shall establish procedures to verify whether the individual is a child when it is reasonably likely that the organisation will use personal information about a child.

(3) When providing an information society service to a child, an organisation shall not seek to obtain personal information from the child about other individuals, including in particular, personal information relating to the professional activity of parents or guardians, financial information or sociological information except that personal information about the identity and address of the child's parent or guardian may be used for the sole purpose of obtaining the consent under subsection (1).

(4) When complying with its obligations under section 9, an organisation delivering an information society service to a child shall provide a privacy notice that is easily understandable and appropriate to the age of the child.

(5) In legal proceedings brought against an organisation for failure to comply with a requirement of this section, it is a defence for the organisation to prove that it had taken such care as in all circumstances was reasonably necessary to comply with such requirement.

(6) In this section—

"information society service" means a service which is delivered by means of digital or electronic communications; and

"child" means an individual under the age of 14.

PART 3

RIGHTS OF INDIVIDUALS

Access to personal information

17 (1) Subject to subsections (2) to (4) and to section 18, at the request of an individual for access to his personal information, and having regard to that which is reasonable, an organisation shall provide the individual with access to—

(a) personal information about the individual in the custody or under the control of the organisation;

(b) the purposes for which the personal information has been and is being used by the organisation; and

(c) the names of the persons or types of persons to whom and circumstances in which the personal information has been and is being disclosed.

(2) An organisation may refuse to provide access to personal information under subsection (1) if—

(a) the personal information is protected by any legal privilege;

(b) the disclosure of the personal information would reveal confidential information of the organisation or of a third party that is of a commercial nature and it is not unreasonable to withhold that information;

(c) the personal information is being used for a current disciplinary or criminal investigation or legal proceedings, and refusal does not prejudice the right of the individual to receive a fair hearing;

(d) the personal information was used by a mediator or arbitrator, or was created in the conduct of a mediation or arbitration for which the mediator or arbitrator was appointed to act under an agreement or by a court;

(e) the disclosure of the personal information would reveal the intentions of the organisation in relation to any negotiations with the individual to the extent that the provision of access would be likely to prejudice those negotiations.

(3) An organisation shall not provide access to personal information under subsection (1) if—

(a) the disclosure of the personal information could reasonably be expected to threaten the life or security of an individual;

(b) the personal information would reveal personal information about another individual; or

(c) the personal information would reveal the identity of an individual who has in confidence provided an opinion about another individual and the individual providing the opinion does not consent to disclosure of his identity,

unless it is reasonable in all the circumstances to provide access.

(4) If an organisation is reasonably able to redact the information referred to in subsection (2)(b) or (3)(b) or (c) from the personal information about the individual who requested it, the organisation shall provide the individual with access to his personal information after redacting the former information.

Access to medical records

18 (1) On the request of an individual for access to—

(a) personal information of a medical or psychiatric nature relating to the individual; or

(b) personal information kept for the purposes of, or obtained in the course of, the carrying out of social work in relation to the individual,

an organisation may refuse to provide access to personal information if disclosure of the personal information to the individual would be likely to prejudice the physical or mental health of the individual.

(2) Where, under subsection (1), an organisation refuses to grant a request, the organisation shall, if requested to do so by the individual, provide access to personal information referred to in that subsection to a health professional, within the meaning of section 2 of the Bermuda Health Council Act 2004, who has expertise in relation to the subject matter of the record, and the health professional shall determine whether disclosure

of the personal information to the individual would be likely to prejudice the physical or mental health of the individual.

(3) Notwithstanding anything else in this section, in response to a request under subsection (1), an organisation—

(a) may refuse to provide access to personal information by relying on section 17(2); and

(b) shall refuse to provide access to personal information pursuant to section 17(3).

(4) If an organisation is reasonably able to redact information which is referred to in section 17(2)(b) or section 17(3)(b) or (c) or information which would be likely to prejudice the physical or mental health of the individual from other personal information about the individual who requested it, the organisation shall provide the individual with access to the other personal information after redacting the former information or the information which would be likely to prejudice the physical or mental health of the individual.

Rectification, blocking, erasure and destruction

19 (1) An individual may make a written request to an organisation to correct an error or omission in any of his personal information which is under the control of the organisation.

(2) If there is an error or omission in personal information in respect of which a request for a correction is received by an organisation under subsection (1), the organisation shall—

(a) correct the personal information as soon as reasonably practicable; and

(b) where the organisation has disclosed the incorrect information to other organisations, send a notification containing the corrected information to each organisation to which the incorrect information has been disclosed, if it is reasonable to do so.

(3) On receiving notification under subsection (2)(b) containing corrected personal information, an organisation shall correct the personal information.

(4) An organisation shall obtain the consent of the writer of an opinion, including a professional or expert opinion, before making a correction to or otherwise altering such opinion.

(5) If consent is not provided under subsection (4), the organisation shall note what is contained in the individual's written request to change any error or omission in the opinion in a manner that links that request with that opinion.

(6) An individual may request an organisation to cease, or not to begin, using his personal information for the purposes of advertising, marketing or public relations.

(7) On receiving a request under subsection (6), an organisation shall cease, or not begin, using the personal information for the purposes of advertising, marketing or public relations.

(8) An individual may request an organisation to cease, or not to begin, using his personal information where the use of that personal information is causing or is likely to cause substantial damage or substantial distress to the individual or to another individual.

(9) On receiving a request under subsection (8), an organisation shall either cease, or not begin, using the personal information that the individual has identified in his request, or provide the individual with written reasons as to why the use of such personal information is justified.

(10) An individual may request an organisation to erase or destroy personal information about the individual where that personal information is no longer relevant for the purposes of its use.

(11) On receiving a request under subsection (10), an organisation shall erase or destroy the personal information that the individual has identified in his request, or provide the individual with its written reasons as to why the use of such personal information is justified.

Procedure for making a request under section 17, 18 or 19

20 (1) In order to obtain access to his personal information or make a request for a correction to his personal information, the individual (in this section referred to as the "applicant") shall make a written request to the organisation setting out sufficient detail to enable the organisation, with a reasonable effort, to identify the personal information in respect of which the request is made.

(2) The applicant may ask for a copy of his personal information or ask to examine his personal information.

(3) An organisation shall promptly acknowledge in writing receipt of a request, including the date of the request, and the organisation shall at the same time inform the applicant, if there is insufficient detail in the request, what information is required to complete his request.

(4) Subject to subsection (5), when a completed request has been received, an organisation shall respond to an applicant not later than—

(a) 45 days from the day on which the organisation receives the applicant's written request referred to in subsection (1); or

(b) the end of an extended time period if the time period is extended under subsection (6).

(5) An organisation is not required to comply with subsection (4) whilst any requests to the Commissioner made by the applicant or organisation regarding the scope of rights or obligations pertaining to the applicant's request under section 17, 18 or 19 are pending.

(6) An organisation may, with respect to a request made under section 17, 18 or 19, extend the period for responding to the request by no more than 30 days, or for such longer period as the Commissioner may permit, if—

(a) a large amount of personal information is requested or needs to be searched or corrected;

(b) meeting the time limit would unreasonably interfere with the operations of the organisation; or

(c) more time is needed to consult with a third party before the organisation is able to determine whether or not to give the applicant access to the requested personal information.

(7) If the period for responding is extended under subsection (6), the organisation shall inform the applicant of the following—

(a) the reason for the extension; and

(b) the time when a response from the organisation can be expected.

(8) An organisation may charge an applicant who makes a request under section 17 or 18 a fee not exceeding the prescribed maximum for access to the applicant's personal information, except where any such request results in the correction of an error or omission in the personal information about the individual that is under the control of the organisation.

(9) A fee may not be charged under subsection (8) if the organisation is prevented from charging such a fee by its professional regulatory body.

(10) If an organisation is intending to charge an applicant a fee for a service, the organisation may require the applicant to pay all or part of the fee in advance, as determined by the organisation.

(11) The Minister may, in consultation with the Commissioner, prescribe any applicable fees.

(12) An organisation is not required to comply with section 17, 18 or 19 of this Act if the request is manifestly unreasonable.

(13) If an organisation refuses to take action at the request of an applicant, the organisation shall inform the applicant in writing of the reasons for the refusal and of the right to contact the Commissioner to make a complaint.

Compensation for financial loss or distress

21 (1) An individual who suffers—

(a) financial loss; or

(b) emotional distress,

by reason of failure to comply with any of the requirements of this Act by an organisation is entitled to compensation from the organisation.

(2) In legal proceedings brought against an organisation for failure to comply this Act, it is a defence for the organisation to prove that it had taken such care as in all circumstances was reasonably necessary to comply with the requirement.

(3) The amount of compensation that an individual is entitled to under this section for each contravention shall be determined by the court.

PART 4

EXEMPTIONS

National security exemption

22 (1) Except for the minimum requirements, Parts 2 and 3 do not apply to the use of personal information required for the purpose of safeguarding national security.

(2) In order to rely on subsection (1), an organisation shall first obtain a certificate ("an exemption certificate") signed by the Minister, in consultation with the Minister responsible for national security, certifying that an exemption from all or any of the provisions of Parts 2 and 3, other than the minimum requirements, is required for that purpose.

(3) The Minister shall not sign an exemption certificate unless satisfied that the exemption is necessary and proportionate for the purpose of safeguarding national security.

(4) An exemption certificate may identify the personal information to which it applies by means of a general description and shall be expressed to have prospective effect.

(5) An individual or organisation directly affected by the Minister's decision whether or not to issue an exemption certificate may appeal to the Supreme Court against the Minister's decision.

Communication provider exemption

23 (1) An organisation that acts as a communication provider and its directors, officers or authorised agents are not liable under this Act for any breach committed while acting as a communication provider.

(2) In this section "communication provider" means an internet service provider, telecommunications and such other organisation that acts as a conduit for personal information transmitted by a third party and who does not determine the purpose of using that personal information.

Regulatory activity and honours exemption

24 (1) Except for the minimum requirements, Parts 2 and 3 of this Act do not apply to the use of personal information if such use is required for the purposes of discharging functions to which this subsection applies to the extent to which the application of those Parts would be likely to prejudice the proper discharge of those functions.

(2) Subsection (1) applies to any relevant function which is designed—

(a) to protect members of the public against—

(i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness, impropriety or professional incompetence of, individuals concerned in the provision of banking,

insurance, investment, trust or other financial services or in the management and ownership of an organisation;

(ii) financial loss due to the conduct of discharged or undischarged bankrupts; or

(iii) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or professional incompetence of, individuals authorised to carry on any profession or other activity;

(b) to protect charities against misconduct or mismanagement (whether by trustees or other persons) in their administration;

(c) to protect the property of charities from loss or misapplication, or to recover such property;

(d) to secure the health, safety and welfare of individuals at work; or

(e) to protect the public against risk to their health or safety arising out of or in connection with the actions of individuals at work.

(3) In subsection (2), "relevant function" means—

(a) any function conferred on any person by or under any statutory provision;

(b) any function of the Crown, a Minister of the Crown or a government department; or

(c) any other function which is of a public nature and is exercised in the public interest.

(4) Parts 2 and 3 of this Act, except for the minimum requirements, do not apply to the use of personal information if such use is required for the purposes of the conferring by the Crown or Premier of any honour or dignity.

General exemption

25 Except for the minimum requirements, Parts 2 and 3 of this Act do not apply to the use of personal information in any case where such use is required for—

(a) the prevention or detection of crime and compliance with international obligations regarding the detection, investigation and prevention of crime;

(b) the apprehension or prosecution of offenders;

(c) the assessment or collection of any tax or duty;

(d) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professionals; or

(e) the economic or financial interests of Bermuda, including monetary, budgetary and taxation matters, compliance with international tax treaties and any monitoring, inspection or regulatory function exercised by official authorities for monetary, budgetary and taxation purposes in Bermuda,

to the extent that the application of those Parts would be likely to prejudice any of the matters mentioned in this section.

PART 5

SUPERVISION

Establishment and appointment of the Commissioner

26 (1) The office of Privacy Commissioner is established as a public office.

(2) The Commissioner shall be appointed by the Governor after consultation with the Premier, who shall first have consulted with the Opposition Leader.

(3) The Commissioner shall be appointed for a period of five years and may be reappointed for a further period of five years, except for the first appointment after the commencement of this Act which may be for a shorter period where the Minister considers that to be expedient.

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

(5) Subject to such exceptions as the Governor acting in his discretion may authorise in writing, the Commissioner shall not hold any office of profit other than that of Commissioner or otherwise engage in any occupation for reward outside the duties of the Privacy Commissioner.

Staff

27 (1) There shall be appointed to assist the Commissioner in the discharge of his functions such number of public officers as may be required.

(2) The Commissioner may, in addition, engage from time to time such technical or professional advisers as he considers necessary to assist in the discharge of his functions under this Act.

(3) Every person appointed or engaged under this section is subject to the Commissioner's direction and control in the performance of functions under this Act.

Funding for office and accounting

28 (1) All salaries, allowances and other expenditure payable or incurred under this Act shall be payable out of money appropriated by the Legislature for that purpose.

(2) The Commissioner is designated as controlling officer in respect of estimates of expenditure approved in relation to the office of Commissioner.

(3) The Commissioner shall cause proper accounts to be kept and maintained of all the financial transactions with respect to the office of Commissioner and shall prepare in respect of each financial year a statement of such accounts in such form as the Accountant General may direct.

(4) The accounts of the office of Privacy Commissioner shall be audited and reported on annually by the Auditor General, and for that purpose the Auditor General or any person authorised by him shall have access to all books, records, returns and other documents relating to such accounts.

General powers of the Commissioner

29 (1) The Commissioner is responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may—

(a) conduct investigations concerning compliance with any provision of this Act;

(b) make an order described in section 44 on completing an investigation whether or not a review is requested or an inquiry completed;

(c) educate the public about this Act;

(d) receive comments from the public concerning the administration of this Act;

(e) engage in, or commission, research into anything affecting the achievement of the purposes of this Act;

(f) comment on the implications for protection of personal information in relation to an organisation's existing or proposed programmes;

(g) approve binding corporate rules for transfers of personal information to an overseas third party under section 15 when the Commissioner considers the binding corporate rules provide a comparable level of protection for personal information as the protection required by this Act

(h) issue formal warnings, admonish an organisation and bring to its attention any failure by the organisation to comply with this Act or agree a course of action with an organisation;

(i) give guidance and recommendations of general application to an organisation on matters relating to its rights or obligations under this Act;

(j) liaise and co-operate with domestic and foreign law enforcement agencies and regulators to the extent necessary to ensure that the purposes of this Act are achieved provided that there is no contravention of the Act;

(k) make recommendations to the Minister concerning the designation of any jurisdiction as providing a comparable level of protection for the purposes of section 15;

(l) make an order at his discretion to permit an organisation to transfer personal information to an overseas third party for use either on behalf of the organisation or for that overseas third party's own business practices, where the organisation has reasonably demonstrated that it is unable to comply with section 15(2) provided the transfer does not undermine the rights of the individual;

(m) establish or assist with the establishment of certification mechanisms and associated rules for the purpose of demonstrating compliance with this Act and may, without prejudice to his tasks and powers under this Act, delegate the operation of a certification mechanism to an independent certification body with the appropriate level of expertise in relation to the protection of personal information;

(n) charge such fees as he thinks fit for any services provided under this Act, not exceeding the prescribed maximum;

(o) do anything which reasonably appears to him to be incidental or conducive to the carrying out of his functions under this Act.

(2) Without limiting subsection (1), the Commissioner may investigate and attempt to resolve complaints that—

(a) an obligation imposed on an organisation by this Act has not been performed;

(b) a right set out in this Act has not been observed;

(c) personal information has been used by an organisation contrary to this Act;

(d) an organisation is not in compliance with this Act.

(3) On receipt of a request from an organisation for an assessment of the organisation's compliance, or intended compliance, with all or any part of its obligations under this Act, the Commissioner may provide a finding or decision in response to the request.

(4) When the Commissioner considers that there may have been or could be a breach of this Act, the Commissioner may serve an organisation with a notice requiring the organisation, within such time as is specified in the notice, to provide the Commissioner, in such form as may be specified, with such information as is specified in the notice.

(5) On receipt of a notice under subsection (4), the organisation shall comply with the requirements in the notice save for communications between the organisation and its professional legal advisers in connection with the giving or receiving of legal advice or made in contemplation of proceedings under or arising out of this Act.

Power to authorise an organisation to disregard certain requests

30 In response to a written request by an organisation, the Commissioner may authorise the organisation to disregard one or more requests made under sections 17, 18 or 19 if, because of their repetitious or systematic nature, the requests would unreasonably interfere with the operations of the organisation or amount to an abuse of the right to make those requests or are otherwise frivolous or vexatious.

Powers concerning investigations and inquiries

31 (1) In conducting an investigation under section 29 or an inquiry under section 42, the Commissioner has all the powers, privileges and immunities of a commissioner

under the Commissions of Inquiry Act 1935 and the powers given by subsection (2) of this section.

(2) The Commissioner may make an order requiring any information relevant to an investigation or inquiry to be produced to him, and may examine any such information, including personal information, whether or not the information is subject to this Act.

(3) Notwithstanding any other enactment or any privilege of the law of evidence, but subject to any claim for legal professional privilege, an organisation shall produce to the Commissioner within ten days any information or a copy of any information required under subsection (1) or (2).

(4) If an organisation is required to produce information under subsection (1) or (2) and it is not reasonable to make a copy of the information, the organisation may require the Commissioner to examine the original information at its premises.

(5) If a judge of the Supreme Court is satisfied by information supplied by the Commissioner that there are reasonable grounds for suspecting—

(a) that an organisation has contravened or is contravening any provision in this Act; or

(b) that an offence under this Act has been committed,

he may grant a warrant to the Commissioner for the Commissioner to enter any premises occupied by an organisation to examine or obtain copies of information containing any matter relevant to the investigation or inquiry.

(6) After completing an inquiry or investigating a complaint, the Commissioner shall return any information or any copy of any information produced.

(7) The Commissioner may publish any finding or decision in a complete or an abridged form.

(8) In the event that a claim for legal professional privilege under this section is disputed by any party, the relevant material shall be sealed and held by a neutral party and the party claiming privilege shall bring the matter before the Supreme Court no later than ten business days following such claim.

Codes of practice

32 (1) The Minister shall, following consultation with the Commissioner, establish codes of practice providing best practice advice for organisations generally, or for specific types of organisation, to comply with this Act.

(2) In the course of preparing a code of practice, the Minister shall consult with relevant individuals and organisations.

(3) The Minister shall arrange for the publication and dissemination of codes of practice to such persons as he considers appropriate.

(4) A failure on the part of any person to act in accordance with any provision of a code of practice does not of itself render that person liable to any legal proceedings in any court or tribunal.

(5) If any provision of the code of practice appears to—

(a) a court conducting any proceedings under this Act;

(b) a court conducting any other legal proceedings; or

(c) the Commissioner carrying out any function under this Act,

to be relevant to any question arising in the proceedings or in connection with the exercise of that jurisdiction or in the carrying out of those functions, in relation to any time when it was in force, that provision of the code of practice shall be taken into account in determining that question.

(6) Codes of practice issued under this Act are not statutory instruments and the Statutory Instruments Act 1977 shall not apply to them.

Statements not admissible for prosecution

33 (1) Any written statement provided by an individual in response to a notice served on an organisation by the Commissioner under section 29(4) may not be used in evidence against that person except—

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

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

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

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

Restrictions on disclosure of information

34 (1) The Commissioner, and any person acting for him or under his direction, shall not disclose any information obtained in performing his duties, powers and functions under this Act, except as provided in this section.

(2) The Commissioner may disclose, or authorise anyone acting for him or under his direction to disclose, information that is necessary for the purposes of—

(a) conducting an investigation or inquiry under this Act;

(b) establishing the grounds for findings and recommendations contained in a report under this Act; or

(c) providing guidance about compliance with the Act relating to good and bad practice by organisations.

(3) In conducting an investigation or inquiry under this Act and in a report under this Act, the Commissioner and anyone acting for him or under his direction shall—

(a) not disclose to any individual any personal information that an organisation would be required to refuse access to; and

(b) take every reasonable precaution to avoid disclosing to any individual any personal information that an organisation would be permitted to refuse to access to,

if access to personal information was requested under sections 17 or 18

(4) The Commissioner may disclose, or authorise anyone acting for him or under his direction to disclose, information in the course of a prosecution, application or appeal under this Act.

(5) The Commissioner may disclose, or authorise anyone acting for him or under his direction to disclose, information relating to the commission of an offence to the Director of Public Prosecutions if the Commissioner considers that there is evidence of an offence under this Act.

(6) This section applies—

(a) to a former Commissioner as it applies to the Commissioner, except that only the Commissioner may authorise a person to make a disclosure; and

(b) to a person formerly acting for or under the direction of the Commissioner or a former Commissioner as it applies to a person currently acting for or under the direction of the Commissioner.

Protection of the Commissioner and staff

35 No proceedings shall lie against the Commissioner or a former Commissioner, or against anyone acting for or under the direction of the Commissioner or a former 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 Act.

Delegation by the Commissioner

36 (1) The Commissioner may delegate in writing to any member of his staff any duty, power or function of the Commissioner under this Act, except the power to delegate.

(2) A delegation under subsection (1) may contain any conditions or restrictions the Commissioner considers appropriate.

Reports by the Commissioner

37 (1) The Commissioner shall, within three months after the end of each calendar year, prepare a report on—

(a) the work of the Commissioner's office under this Act; and

(b) any other matters relating to protection of personal information that the Commissioner considers appropriate.

(2) The Commissioner shall cause copies of the annual report to be laid before each House of the Legislature.

(3) The Commissioner may from time to time cause copies of a report to be laid before each House of the Legislature with respect to his functions as the Commissioner thinks fit.

Right to ask for a review or initiate a complaint

38 (1) An individual who makes a request to an organisation respecting his personal information may ask the Commissioner to review the organisation's decision, action or failure to act.

(2) An individual may initiate a complaint with respect to the matters referred to in section 29(2).

(3) If the Commissioner is satisfied that there are other grievance, complaint or review procedures available for the purposes of resolving matters for which a review may be requested or a complaint may be initiated under this Part, the Commissioner may require that the person first exhaust those other procedures with a view to resolving the matter before the Commissioner proceeds to hear or otherwise deal with the review or complaint.

Procedure for a review or initiating a complaint

39 (1) To ask for a review or to initiate a complaint under this Part, an individual shall deliver a written request to the Commissioner.

(2) A written request to the Commissioner for a review of a decision of an organisation shall be delivered within—

(a) 30 days from the date on which the individual asking for the review is notified of the decision; or

(b) such longer period as may be allowed by the Commissioner.

(3) A written request to the Commissioner initiating a complaint shall be delivered within a reasonable time.

(4) The time limit in subsection (2)(a) does not apply to delivering a written request for a review concerning an organisation's failure to respond within a required time period.

(5) The Commissioner may disregard a request made under this section if the Commissioner believes the request is without merit or where there is insufficient evidence to proceed.

Notifying others of review or complaint

40 (1) On receiving a written request for a review, the Commissioner shall give a copy to—

(a) the organisation concerned; and

(b) any other person that the Commissioner considers appropriate.

(2) On receiving a written request initiating a complaint, the Commissioner shall give a copy to—

(a) the organisation concerned; and

(b) any other person that the Commissioner considers appropriate.

(3) The Commissioner may redact any information contained in the written request that the Commissioner considers appropriate before giving a copy of the written request to the organisation or any other individual affected by the request.

Mediation

41 (1) The Commissioner may at any time attempt to have a matter that is the subject of an application for review or complaint resolved by negotiation, conciliation, mediation or otherwise.

(2) The Commissioner may authorise any person appointed or engaged under section 27to act as a mediator in any mediation.

(3) Participation in the mediation is voluntary and any party to it may withdraw at any time.

(4) The mediator may decide to terminate the meditation at any time, in which case the mediator shall provide written reasons for so deciding.

(5) Anything said or admitted during the mediation and any document prepared for the purposes of the mediation shall not be admissible in evidence against any person in any subsequent proceeding concerning a matter that is the subject of the mediation, and no evidence in respect of the mediation may be given against any person.

Inquiry by the Commissioner

42 (1) If a matter under review or relating to a complaint is not resolved by mediation under section 41 or otherwise, the Commissioner may conduct an inquiry and decide all questions of process, fact and law arising in the course of the inquiry.

(2) An inquiry under subsection (1) may be conducted in private if the Commissioner considers it to be necessary.

(3) A person who asks for a review or initiates a complaint, the organisation concerned and any person given a copy of the written request for the review or initiating the complaint—

(a) shall be given an opportunity to make representations to the Commissioner during the inquiry; and

(b) may be represented at the inquiry by a lawyer or an agent.

(4) The Commissioner may decide—

(a) whether representations are to be made orally or in writing; and

(b) whether a person is entitled to be present during, or to have access to or to comment on, representations made to the Commissioner by another person.

(5) An inquiry into a matter that is the subject of a written request referred to in section 39 shall be completed within six months from the date on which the written request was received by the Commissioner, unless the Commissioner—

(a) notifies the person who made the written request, the organisation concerned and any other person given a copy of the written request that the Commissioner is extending that period; and

(b) provides an anticipated date for the completion of the review.

(6) If requested by either a person who asks for a review or initiates a complaint or an organisation concerned, the Commissioner shall provide written reasons for arriving at his decisions when conducting an inquiry.

Burden of proof

43 At an inquiry into a decision under which an individual was refused—

(a) access to all or part of his personal information; or

(b) information concerning the use of his personal information,

it is for the organisation to establish to the satisfaction of the Commissioner that the individual has no right of access to his personal information or no right to the information concerning the use of his personal information.

Commissioner's orders

44 (1) On completing an inquiry under section 42, the Commissioner shall dispose of the matters by making an order under this section or issuing a formal warning or public admonishment.

(2) If the inquiry relates to an organisation's decision to give or refuse to give access to all or part of an individual's personal information, the Commissioner may, by order—

(a) direct the organisation to give the individual access to all or part of his personal information that is under the control of the organisation if the Commissioner determines that the organisation is not permitted under this Act to refuse access;

(b) confirm the decision of the organisation or require the organisation to reconsider its decision concerning access if the Commissioner determines that the organisation may under this Act refuse access; or

(c) direct the organisation to refuse the individual access to all or part of his personal information if the Commissioner determines that the organisation is required under this Act to refuse access.

(3) If the inquiry relates to any other matter, the Commissioner may, by order, do one or more of the following—

(a) confirm that an obligation imposed on an organisation by this Act has been performed or require that an obligation imposed on an organisation by this

Act be performed, including requiring an organisation to take specific steps to remedy a breach of this Act;

(b) confirm that a right set out in this Act has been observed or require that a right set out in this Act be observed;

(c) confirm a decision not to correct, erase, delete or destroy personal information or specify that personal information is to be corrected, erased, deleted or destroyed and how such personal information is to be corrected, erased, deleted or destroyed and may, if reasonably practicable, require the organisation to notify third parties to whom the personal information has been disclosed of the correction, erasure, deletion or destruction;

(d) require an organisation to stop using personal information in contravention of this Act;

(e) confirm a decision of an organisation to use personal information;

(f) require an organisation to destroy personal information used contrary to this Act;

(g) require an organisation to provide specific information to persons in the event of a breach under section 14(1) which is likely to cause significant harm to individuals.

(4) In the event that an order under subsection (2) or (3) would not be applicable, the Commissioner may make such order as he considers appropriate, or may issue a formal warning or public admonishment.

(5) The Commissioner may specify any terms or conditions in an order made under this section.

(6) The Commissioner shall give a copy of an order made under this section to—

(a) the person who asked for the review or initiated the complaint;

(b) the organisation concerned;

(c) any person given a copy of the written request under section 40; and

(d) the Minister.

(7) A copy of an order made by the Commissioner under this section may be filed with the Registrar of the Supreme Court and, after filing, the order is enforceable as a judgment or order of that Court.

Judicial review

45 (1) Subject to subsection (2), not later than 50 days from the day that an organisation is given a copy of an order of the Commissioner, the organisation concerned shall comply with the order.

(2) Any person aggrieved by a decision of the Commissioner under this Act may apply to the Supreme Court for a review of the decision and the Court, after considering the application, may confirm, vary, remit or set aside the decision.

(3) An application under subsection (2) shall be made not later than 45 days from the day the organisation making the application is given a copy of the order.

(4) If an application for judicial review is made pursuant to subsection (2), the Commissioner's order is stayed until the application is dealt with by the court.

(5) The court may, on application made either before or after the expiry of the period referred to in subsection (3), extend that period if the court considers it appropriate to do so.

PART 6

GENERAL PROVISIONS

Disclosure for purposes of business transaction

46 (1) In this section—

(a) "business transaction" means a transaction consisting of the purchase, sale, lease, merger or amalgamation or any other type of acquisition or disposal of, or the taking of a security interest in respect of, an organisation or a portion of an organisation or any business or activity or business asset of an organisation and includes a prospective transaction of such a nature;

(b) "party" includes a prospective party.

(2) Notwithstanding any other provision of this Act, an organisation may, for the purposes of a business transaction between itself and one or more other organisations, use personal information in accordance with this section.

(3) Organisations that are parties to a business transaction may—

(a) during the period leading up to and including the completion, if any, of the business transaction, use personal information about a person without the consent of the person provided that all the following conditions are satisfied—

(i) the parties have entered into an agreement under which the use of the personal information is restricted to those purposes that relate to the business transaction; and

(ii) the personal information is necessary—

(A) for the parties to determine whether to proceed with the business transaction; and

(B) if the determination is to proceed with the business transaction, for the parties to carry out and complete the business transaction; and

(b) where the business transaction is completed, use personal information about a person without the consent of the person if—

(i) the parties have entered into an agreement under which the parties undertake to use and disclose the personal information only for those purposes for which the personal information was initially collected from or in respect of those persons; and

(ii) the personal information relates solely to the carrying on of the business or activity or the carrying out of the objects for which the business transaction took place.

(4) If a business transaction does not proceed or is not completed, the party to whom the personal information was disclosed shall, if the personal information is still in the custody of or under the control of that party, either destroy the personal information or turn it over to the party which disclosed the personal information.

(5) Nothing in this section is to be construed so as to restrict a party to a business transaction from obtaining the consent of a person to the use of personal information about the person for purposes beyond the purposes for which the party obtained the personal information under this section.

(6) This section does not apply to a business transaction where the primary purpose, objective or result of the transaction is the purchase, sale, lease, transfer, disposal or disclosure of personal information.

Offences and penalties

47 (1) Subject to subsection (5), a person commits an offence if he—

(a) wilfully or negligently uses or authorises the use of personal information in a manner that is inconsistent with Part 2 and is likely to cause harm to an individual or individuals ;

(b) wilfully attempts to gain or gains access to personal information in a manner that is inconsistent with this Act and is likely to cause harm to an individual or individuals;

(c) disposes of or alters, falsifies, conceals or destroys personal information, or directs another person to do so, in order to evade a request for access to the personal information;

(d) obstructs the Commissioner or an authorised delegate of the Commissioner in the performance of the Commissioner's duties, powers or functions under this Act;

(e) knowingly makes a false statement to the Commissioner or knowingly misleads or attempts to mislead the Commissioner in the course of the Commissioner's performance of the Commissioner's duties, powers or functions under this Act;

(f) knowingly or recklessly fails to comply with section34(1) (restrictions on disclosure by Commissioner or staff).

(2) Subject to subsections (4) and (5), a person commits an offence if he—

(a) fails to comply with an order made by the Commissioner under this Act;

(b) fails to comply with a notice served by the Commissioner under this Act;

(c) contravenes section 7 (sensitive personal information);

(d) disposes of, alters, falsifies, conceals or destroys evidence during an investigation or inquiry by the Commissioner; or

(e) fails to notify a breach of security to the Commissioner in accordance with section 14 of this Act.

(3) A person who commits an offence under subsection (1) or (2) is liable—

(a) on summary conviction, in the case of an individual, to a fine not exceeding $25,000 or to imprisonment not exceeding two years or to both.; and

(b) on conviction on indictment, in the case of a person other than an individual, to a fine not exceeding $250,000.

(4) In proceedings brought against an organisation or an individual, it is a defence for the organisation or individual charged with an offence under subsection (2) to prove to the satisfaction of the court that the organisation or individual, as the case may be, acted reasonably in the circumstances that gave rise to the offence.

(5) In determining whether a person has committed an offence under this Act, a court shall consider whether a person has followed any relevant code of practice which was at the time issued by the Minister.

(6) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of, or to be attributable to, any neglect on the part of—

(a) any director, manager, secretary or similar officer of the body corporate; or

(b) any person who was purporting to act in any such capacity,

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

(7) Where the affairs of a body corporate are managed by its members, subsection (6) applies, in relation to the acts and defaults of a member in connection with his functions of management, as if he were a director of the body corporate.

Power to make regulations

48 (1) The Minister may, in consultation with the Commissioner, make regulations generally for the carrying out of or giving effect to the purposes of this Act, and may prescribe anything required or permitted to be prescribed under this Act.

(2) The negative resolution procedure shall apply to regulations made under this Act.

Review of the Act

49 The Minister shall carry out a comprehensive review of this Act within five years of its coming into operation, and shall submit a report to the House of Assembly within 18 months after beginning the review.

Crown application

50 This Act binds the Crown.

Power to make consequential amendments

51 The Minister may, by regulations, make consequential amendments to the Public Access to Information Act 2010 and to other Acts that appear to the Minister to be necessary or expedient for the purposes of this Act.

Commencement

52 (1) This Act comes into operation on a day to be appointed by the Minister by notice published in the Gazette.

(2) The Minister may appoint different days for different provisions of the Act.

PERSONAL INFORMATION PROTECTION BILL 2016

EXPLANATORY MEMORANDUM

This Bill seeks to regulate the use of personal information by organisations in a manner which recognises both the need to protect the rights of individuals in relation to their personal information and the need for organisations to use personal information for legitimate purposes

Clause 1 provides the title of the Bill.

Clause 2 sets out various definitions and interpretive provisions.

Clause 3 provides that the Act applies to every organisation that uses personal information by automated means and personal information used other than by automated means that forms part of a structured filing system.

Clause 4 provides the types of personal information excluded from the Act.

Clause 5 provides that an organisation is responsible for adopting policies that give effect to its obligations and the rights of individuals provided in the Act.

Clause 6 sets out the conditions in when an organisation may use an individual's personal information.

Clause 7 provides the meaning of sensitive personal information and that sensitive personal information cannot be used to discriminate against an individual contrary to the provisions of the Human Rights Act 1981.

Clause 8 provides that an organisation can only use personal information in a lawful and fair manner.

Clause 9 provides that an organisation shall provide individuals with a privacy notice about its practices and policies regarding personal information.

Clause 10 provides that an organisation can only use personal information for specific purposes as set out in the Act.

Clause 11 provides that an organisation shall only use personal information that is relevant to the purpose for which that personal information is used.

Clause 12 provides that an organisation must ensure that any personal information used is accurate and up-to-date and is not kept for longer than is necessary.

Clause 13 provides that an organisation must have appropriate safeguards in place to protect personal information.

Clause 14 sets out the obligations an organisation shall fulfil if there is a breach of security at the organisation regarding personal information.

Clause 15 provides the responsibilities of an organisation when transferring personal information to an overseas third party.

Clause 16 provides that when using the personal information of a child in an information society service targeted at children or when there is knowledge that the personal information used is that of a child, an organisation shall obtain the consent from a parent or guardian before the child's personal information is collected.

Clause 17 sets out when an organisation may refuse to give access an individual requesting access to his personal information.

Clause 18 provides when an organisation may give an individual access to his medical records.

Clause 19 provides that an individual may, by written request to an organisation, seek to have an error or omission in his personal information corrected and an organisation's obligations regarding the request.

Clause 20 sets out the procedure for making a request under clauses 17, 18 or 19 of the Bill.

Clause 21 provides that an individual is entitled to compensation from an organisation if he suffers a loss or distress due the organisation's failure to comply with the Act

Clause 22, 23, 24 and 25 provide the various exemptions for the use of personal information in the interest of national security, for communication providers, regulatory and honours purposes and generally.

Clause 26 provides the establishment of the office of Privacy Commissioner as a public office and the appointment of the Commissioner.

Clause 27 makes provision for the appointment of staff.

Clause 28 provides for the funding and accounting for the office of Privacy Commissioner.

Clause 29 provides the general powers of the Commissioner.

Clause 30 gives the Commissioner the power to authorise an organisation to disregard one or more requests made under clauses 17, 18 or 19 of the Bill.

Clause 31 sets out the Commissioners powers concerning investigations and inquiries.

Clause 32 requires the Minister, in consultation with the Commissioner, to establish codes of practice to organisations regarding the administration of this Act.

Clause 33 provides which written statements are not admissible for prosecution.

Clause 34 provides that the Commissioner or a person acting for or under his direction must not disclose information obtained when performing his duties and functions under the Act.

Clause 35 provides for the protection of the Commissioner and staff of the office of Privacy Commissioner.

Clause 36 provides that the Commissioner may delegate any of his duties or functions to any member of staff of the office of Privacy Commissioner.

Clause 37 provides for reports by the Commissioner and that such reports shall be laid before the Houses of the Legislature.

Clause 38 provides that an individual who makes a request regarding his personal information to an organisation may ask the Commissioner to review a decision made by, or initiate a complaint against, that organisation.

Clause 39 sets out the procedure for a review or initiating a complaint.

Clause 40 provides that the Commissioner shall provide copies of a written request for review to an organisation and any other individual he considers appropriate.

Clause 41 authorises the Commissioner to attempt to mediate a resolution of a matter in respect of which an application has been made.

Clause 42 provides for an inquiry by the Commissioner should a matter under review or relating to a complaint not be resolved by mediation.

Clause 43 provides for the burden of proof at an inquiry into a decision under which an individual was refused access to his personal information or information regarding the use of his personal information.

Clause 44 provides that the Commissioner shall dispose of the matters under review by making an order on completion of an inquiry or issue a formal warning or public admonishment.

Clause 45 provides for judicial review of a decision of the Commissioner.

Clause 46 provides for the disclosure of personal information for the purposes of business transaction.

Clause 47 provides the offences and penalties under the Act.

Clause 48 authorises the Minister to make regulations.

Clause 49 provides for the Minister's comprehensive review of the Act within five years of its coming into operation.

Clause 50 binds the Crown.

Clause 51 gives the Minister the power to make consequential amendments to the Public Access to Information Act 2010 and any other Act deemed appropriate.

Clause 52 provides the commencement of the Act.