Government of Bermuda

The Personal Information Protection Act (PIPA)
Draft Model
For Consultation

GOVERNMENT OF BERMUDA
The Ministry of Economic Development
The Department of E-Commerce

Table of contents

Section **Page**

Explanatory notes

This explanatory note provides some context for the proposed framework for the protection of personal information in Bermuda as detailed in the Personal Information Protection Act Draft Model ("**PIPA Model**").

The framework may be seen as complimentary to the Public Access to Information Act 2010 ("**PATI**"), which provides for public access to Government information. PATI restricts access to personal information and the PIPA Model deals exclusively with personal information, granting individuals more control over the use of their personal information, and requiring organisations to meet certain obligations.

Privacy is the expectation that confidential personal information disclosed in private will not be disclosed to third parties, when that disclosure would cause either embarrassment or emotional distress to a person of reasonable sensitivities. This idea has been developed by a number of international organisations into a set of common principles that embody a right of informational privacy i.e. that everyone has the right to the protection of personal information concerning him or her. These principles have been implemented by a large number of countries and the PIPA Model has been based on them. They are as follows:

1. Personal information shall be used fairly and lawfully.

2. Personal information shall be used for limited specified purposes.

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

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

5. Personal information used for any purpose shall not be kept for longer than is necessary for that use.

6. Personal information shall be used in accordance with the rights of individuals, (as set out in the PIPA Model).

7. Personal information shall be kept securely.

8. Personal information shall only be transferred to third parties (including international transfers) where there is a comparable level of protection.

There have been various attempts at implementing informational privacy in Bermuda. This culminated in a requirement that a new model be developed recognising Bermuda's unique characteristics whilst balancing the needs of business with the desire to provide individuals with suitable protection.

Considerable work has been done to research the current state of informational privacy law in a number of relevant jurisdictions and to extract those elements that would best serve Bermuda. The roots of the Bermuda model stretch from Canada, through the United States to Europe and beyond.

The end result is a draft model that provides a light regulatory environment but which has been prepared so that an application for EU adequacy might be made. EU adequacy would enable the unhindered transfer of personal information between Bermuda and any EU member state together with the increasing number of countries that have also been

deemed adequate by the EU Commission. This would increase economic opportunities for international business operating from Bermuda by helping to satisfy privacy compliance requirements and placing them on a level playing field with those organisations based in many of our competitor jurisdictions that are already deemed adequate.

There has been considerable international activity (and movement) in this sector of the law over the past 10 years. Recent developments have made this a topical area with broad ranging discussions about individual freedoms and commercial interests. Rapid technological developments have also brought new challenges for the protection of personal information.

The scale of data sharing and collecting has increased dramatically. Technology allows both private companies and public authorities to make use of personal information on an unprecedented scale in order to pursue their activities. Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life. Due to all this it is recognised that building trust in the online environment is a key driver to economic development. Lack of trust makes consumers hesitate to buy online and adopt new services. This risks slowing down the economy and growth.

The latest survey undertaken by the Department of E-Commerce showed that ninety-seven percent (97%) of residents consider that the protection of personal information was very important. The overwhelming majority of the stakeholders who have participated in the development of the Bermuda model thought that this was a necessary initiative and would benefit Bermuda and Bermudians.

The Government of Bermuda considers privacy to be a key priority and has decided that the time is now right to introduce a law that protects individual personal privacy while allowing for the proper conduct of business and the operation of government.

Detailed explanation of the proposal

It should be noted that while preparing the PIPA Model, the Department of E-Commerce has undertaken a comprehensive review of similar legislation implemented by other jurisdictions as well as model laws proposed by international bodies.

Part 1 – Interpretation and Scope

The definitions in Section 1 cover the key elements to the legislation. “Organisations” and “use” are drafted broadly. “Personal information” includes personal information held both in manual and electronic form.

Section 2 provides a test of reasonableness. This is a well-known legal concept in Bermuda law and when it is applied, it is intended that a sliding scale will operate dependent on the sensitivity of the personal information, its context and the risk when it is used.

Section 3 states that it covers every organisation that uses personal information held in a structured filing system.

Section 4 identifies the types of circumstances where the provisions of the PIPA Model should not apply. Exclusions are not the same as Exemptions found in Part 4. Exclusions are an ‘absolute’ so that the personal information never falls within the PIPA Model, such as personal information held for domestic purposes. This section includes elements that will enable society, business and government to operate.

The PIPA Model provides additional protection in that it does not allow individuals to contract out of or waive the rights that are granted.

Part 2 – General Principles and Rules

Section 5 states that organisations are always responsible for personal information that they use (even if transferred to third parties) and should take into consideration the privacy implications of the services they provide. They should incorporate these considerations into their policies and procedures at the earliest stage in the development of any new service. This is a concept known as “privacy by design”.

Individuals should be appointed who are responsible for the implementation of the PIPA Model within any organisation. This is someone who other members of staff, the public and the Commissioner can approach if they have a question about the application of the PIPA Model within the organisation.

Section 6 lists the criteria for the use of personal information by organisations. The different criteria listed are broad and cover all those situations that have been found to be necessary over years of use in countries that have implemented this type of legislation. While consent provided by an individual with knowledge of the use to which the personal information might be used is the first option listed, clearly there are situations where consent is not always possible.

Section 7 deals with those areas of personal information that are generally regarded as being “sensitive” such as race, ethnicity, disability, religion and political views; and limits their use so that (save for limited circumstances) an individual may not be discriminated against.

Section 8. Fairness is an accepted principle used by international organisations/countries when dealing with privacy.

Section 9 deals with the notice an organisation must provide to individuals regarding the purpose(s) for which their personal information is used.

Section 10 limits the use of personal information to the purposes the organisation has stated in the notice with some limited exemptions.

Section 11 requires that only relevant personal information be used by an organisation for the stated purpose. This limits the personal information that is collected.

Section 12. Personal information must (when necessary) be maintained up-to-date and not kept for longer than needed.

Section 13 states that personal information must be kept securely, though the level of security should be relevant for the type of personal information held and the potential for harm if the individual's privacy is breached.

Section 14. Any security breach that might adversely affect an individual must be reported to the Commissioner and the relevant individual(s).

Section 15 deals with transfers of personal information to all third parties and, while it does not state this on its face, its main effect relates to international transfers. There are various means by which personal information may be safely transferred and there is an exemption that covers small scale and occasional transfers for the benefit of organisations.

Section 16 deals with personal information relating to children. This is an important area that has resulted in legislation being implemented in the US and EU. Parents or Guardians must be involved in the use of such personal information and where relevant, efforts must be made to ensure that the child understands any notices directed to them.

Part 3 – Rights of Individuals

Section 17 deals with access to personal information by individuals. It describes the process by which this is achieved and states the exemptions that apply.

Section 18 deals with access to medical records.

Section 19 details the rights an individual has to rectify, block, erase or destroy their personal information and the process by which this might be achieved.

Section 20 deals with the procedures for accessing and correcting personal information.

Section 21 deals with compensation for damage and any distress that might have been caused.

Part 4 – Exemptions

Sections 22-25 list the various exemptions from the PIPA Model and include a right for the Government to add further exemptions in the future where necessary so long as the exemption complies with the necessary tests.

Part 5 – Supervision

Sections 26-46 deal with the appointment and role of the Commissioner. The Commissioner oversees the operation of the PIPA Model and has been granted various powers to enable this. While there is a power to conduct investigations (either upon receipt of a complaint from an individual or on his own behalf) and issue reports and fines, a large part of the role is educational. The Commissioner may issue Guidance and help organisations who have queries about the operation of the PIPA Model. The Minister may issue Codes of Practice.

Part 6 – General Provisions

Section 47 enables the limited use of personal information by organisations involved in corporate business transactions.

Section 48 provides for offences and penalties.

Section 49 provides for the Minister, in consultation with the Commissioner, to make Regulations.

Section 50 provides for a review of the PIPA Model.

Section 51 permits the phased introduction of the PIPA Model.

Personal Information Protection Act (PIPA) Draft Model

The purpose of the PIPA is to govern the use of personal information by organisations in a manner that recognises both the need to protect the human rights of individuals in relation to their personal information and the need of organisations to use personal information for purposes that are legitimate.

Part 1 – Interpretation and scope

1. Definitions

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

(b) "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;

(c) "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;

(d) "child" or "children" refers to an individual or group of individuals under 16 years of age;

(e) "Commissioner" means the Privacy Commissioner appointed under this Act;

(f) "company" means any company within the meaning of section 4(1) of the Companies Act 1981, including exempted companies and local companies or any company incorporated by virtue of private Act;

(g) "exempted company" means an exempted company as defined in the Companies Act 1981;

(h) "local company" means a local company as defined in the Companies Act 1981;

(i) "minimum requirements" means the requirements set out in sections 5, 8, 12 and 13;

(j) "Minister" means the Cabinet Minister responsible for this Act;

(k) "organisation" means:

(i) a company,

(ii) an unincorporated association,

(iii) a public authority,

(iv) a partnership, which means any instance where an individual engages in any business in Bermuda as a partner within the meaning of the Partnership Act 1902,

(v) any body incorporated under the law of Bermuda,

(vi) a trade union as defined in section 1(1) of the Trade Union Act 1965, and

(vii) an individual acting in a commercial capacity,

which uses personal information;

(l) “personal information” means any information, electronic or otherwise, about an identified or identifiable individual;

(m) "prescribed maximum" means such amount as may be prescribed by the Minister in regulations;

(n) “public authority” means a public authority as defined in the Interpretation Act 1951;

(o) “publicly available personal information” means personal information about an individual that the individual knowingly makes or permits to be made available to the public, or is legally obtained or accessed from

(i) government records that are available to the public or

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

(p) “transitional period” means the period from … until [*INSERT DATE*]

(q) “use” or “using” means using or carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organising, adapting, altering, retrieving, consulting, disclosing, transferring, disseminating or otherwise making available, combining, blocking, erasing and destroying any personal information.

2. Standard as to what is reasonable

The standard to be applied under this Act in determining whether something is reasonable or unreasonable, or whether a matter has been carried out or otherwise dealt with reasonably or in an unreasonable manner, is that which a reasonable person would consider appropriate in the circumstances.

3. Scope of application

Except as provided in this Act, this Act applies to every organisation that uses personal information in Bermuda and in respect to all personal information used electronically or as part of a structured filing system, where personal information is accessible according to specific criteria for that system.

4. Exclusion from the Act

(1) This Act does not apply to the following:

(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 that individual's capacity as an employee or an official of an organisation;

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

(e) personal information about an individual that has been in existence for at least 100 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 force of this Act;

(g) personal information contained in a court file, used by a judge of the Supreme Court or of the Magistrates Courts, used as part of judicial administration or relating to support services provided to the judges of any of the courts referred to in this subsection, but only where such personal information is necessary for judicial purposes;

(h) personal information used by a Member of the House of Assembly or the Senate, but only where such use relates to the exercise of that official's function and the personal information is covered by parliamentary privilege;

(i) personal information contained in a personal note, communication or draft decision created by or for a person who is acting in a judicial, quasi-judicial or adjudicative capacity.

(2) If an organisation has under its control personal information about an individual that was acquired prior to 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,

(b) may be used and disclosed by the organisation for the purposes for which the personal information was collected, and

(c) after the transitional period, is to be treated in the same manner as personal information collected under this Act.

(3) This Act is not to be applied so as to

(a) affect any legal privilege,

(b) limit the personal information available by law to a party to a legal proceeding, or

(c) limit or affect the use of personal 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 in 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

5. Responsibility and compliance with the Act

(1) Organisations are responsible for adopting suitable measures and policies that give effect to the obligations of organisations and rights of individuals set out in this Act and are encouraged to proactively adopt “privacy by design” and accommodate the privacy interests and rights of individuals in their operations.

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

(3) An organisation must designate a representative for the purposes of compliance with this Act who will have primary responsibility for cooperating with the Commissioner.

(4) An individual designated under subsection (3) may delegate the duties conferred by that designation to one or more individuals.

(5) In meeting its responsibilities under the Act, an organisation must act in a reasonable manner.

6. Criteria for legitimately using personal information

(1) An organisation may use personal information only if one or more of the following conditions are met:

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

(b) a reasonable person giving due weight to the sensitivity of the personal information would consider that the use of the personal information is manifestly in the interests of the individual and consent of the individual cannot be obtained in a timely way, or the individual would not reasonably be expected to withhold consent;

(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 statute or regulation of Bermuda that authorises or requires such use;

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

(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 a current, past or potential employment relationship with the organisation.

(2) Without prejudice to subsection (1), if an organisation cannot meet any of the requirements under subsection (1) then it may use personal information only in the following circumstances:

(a) the personal information was collected from, or is disclosed to, a public authority that is authorised or required by a statute or regulation of Bermuda to provide the personal information to, or collect the personal information from the organisation;

(b) the use of the personal information is for the purpose of complying with an order made by a court, person or body having jurisdiction applicable to 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 adult interdependent partner or to a relative of a deceased individual if, in the opinion of the organisation, the disclosure is appropriate; or

(f) the use of the personal information is reasonable to protect or defend the legitimate interests of the organisation.

(3) This subsection (3) applies only when consent is relied upon under subsection (1) as a criterion for use of personal information.

(a) Organisations must provide individuals with clear, prominent, easily understandable, accessible and affordable mechanisms to give their consent in relation to the use of their personal information.

(b) Organisations are not obliged to provide such mechanisms where it can be reasonably implied from the conduct of individuals that they consent to the use of their personal information for all intended purposes.

(c) When an individual consents to the disclosure of his or her 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 or her personal information for the purpose of coverage or enrolment under an insurance, benefit or similar plan if the individual has an interest in or derives a benefit from that plan.

7. Sensitive Personal information

(1) The personal information referred to in subsection 2 is any personal information relating to categories defined in the Human Rights Act 1981 or such categories as are added to or amended in section 2(2) of that statute.

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

(3) No person shall without lawful authority use personal information relating to the physical or mental health of another person in breach of a duty of confidence.

(4) For the purposes of subsections (2) and (3), personal information is used with lawful authority if and only to the extent that it is used:

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

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

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

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

8. Fairness

Organisations must use personal information in a lawful and fair manner.

9. Notice, transparency and information practices

(1) Organisations must provide clear and easily accessible statements about their practices and policies with respect to personal information and those statements should include:

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

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

(c) the types of persons 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; and

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

(2) Organisations must take all reasonably practicable steps to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon thereafter as is practicable.

(3) Organisations are not obliged to provide the notice required by subsection (1) where either:

(a) the personal information is publicly available personal information; or

(b) all uses made, or to be made, of the personal information are within the reasonable expectations of the individuals to whom the personal information relates.

10. Purpose limitation

Organisations must use personal information only for the specific purposes stated under section 9 or for other compatible or related purposes except:

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

(b) when necessary to provide a service or product required by the individual;

(c) where required by any rule of law or by the order of a 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 personal information is used for the purposes of scientific, statistical or historical research subject to appropriate safeguards for the rights and freedoms of individuals.

11. Proportionality

(1) Organisations must limit the use of personal information to personal information that is relevant for the purposes of such use.

(2) Organisations must ensure that personal information is adequate and not excessive in relation to the purposes for which it is used.

12. Integrity of personal information

(1) Organisations must ensure that any personal information used is accurate and kept up-to-date to the extent necessary for the purposes of use.

(2) Organisations must ensure that personal information used for any purpose or purposes is not kept for longer than is necessary for that purpose or those purposes.

13. Security safeguards

Organisations must protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorised access to personal information, or unauthorised destruction, use, modification or disclosure of personal information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the personal information and the context in which it is held, and should be subject to such reviews and reassessments as are reasonable.

14. Security Breach Notification

(1) In case of a breach of security leading to the accidental loss or unlawful destruction or unauthorised disclosure of or access to personal information which is likely to adversely affect individuals, the organisation responsible for that personal information must, without undue delay, notify the Commissioner of such a breach and shall, after the notification to the Commissioner, communicate such a breach to the affected individuals without undue delay.

(2) The notification to the Commissioner under subsection (1) must describe the nature of the breach and the measures to be taken by the organisation to address the breach.

15. Transfers of Personal Information

(1) When an organisation uses personal information it remains responsible for that personal information, including any transfers of that personal information to a third party for use by that third party on behalf of the organisation, or for the third party's own business purposes. The organisation must assess the level of protection provided by the third party for that personal information and if the organisation reasonably believes that the protection is comparable to that stated under this Act, it may rely on such comparable level of protection while the personal information is being used by that third party. In all other cases, the organisation must employ contractual mechanisms, corporate codes of conduct including binding corporate rules, or other means to provide a comparable level of protection.

(2) To comply with subsection (1), the organisation must consider the level of protection afforded by the law applicable to such third party and the Minister, following a recommendation from the Commissioner, may designate any jurisdiction as providing a comparable level of protection for the purposes of subsection (1).

(3) By way of derogation from subsection (1), an organisation may transfer personal information to a third party for use by that third party, on behalf of the organisation or for the third party's own business purposes, where an organisation assesses all the circumstances surrounding the transfer of personal information to that third party and reasonably considers that the transfer of personal information is small-scale, occasional and is unlikely to prejudice the rights of individuals.

16. Children's Information

(1) Where an organisation uses personal information about a child and consent is relied upon, the organisation must obtain consent from a parent or guardian of the child before the personal information is collected from the child.

(2) An organisation:

(a) must 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) must 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) Organisations must not seek to obtain personal information from a 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 section 9 in respect of a child, organisations must provide statements which are easily understandable and appropriate to the age of the child.

(5) Organisations must comply with their obligations in Part 3 where a parent or guardian exercises any of the rights under Part 3 on behalf of a child, and organisations must establish procedures to verify the identity of a parent or guardian exercising these rights.

(6) In proceedings brought against an organisation by virtue of this section, it is a defence to prove that it had taken such care as in all circumstances was reasonably required to comply with the requirement concerned.

Part 3 – Rights of individuals

17. Access to personal information

(1) Subject to section 18 and subsections (2) to (4), on the request of an individual for access to personal information about the individual, and having regard to that which is reasonable, an organisation must provide the individual with access to the following:

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

(b) the purposes for which the personal information referred to in subsection (1)(a) has been and is being used by the organisation;

(c) the names of the persons or types of persons to whom and circumstances in which the personal information referred to in subsection (1)(a) 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 was collected for a current disciplinary or criminal investigation or legal proceeding and refusal does not prejudice the rights and freedoms of the individual to receive a fair hearing;

(d) the personal information was collected 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:

(i) under an agreement, or

(ii) by a court;

(e) the personal information relates to or may be used in the exercise of prosecutorial discretion; or

(f) the personal information consists of the intentions of the organisation in relation to any negotiations with the individual, to the extent to which the provision of access would be likely to prejudice those negotiations.

(3) An organisation must 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 or her identity

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

(4) If an organisation is reasonably able to sever the information referred to in subsection (2)(b) or (3)(a), (b) or (c) from the personal information about the individual who requested it, the organisation must provide the individual with access to the personal information after the information referred to in subsection (2)(b) or (3)(a), (b) or (c) has been severed.

18. Access to personal information in medical records

(1) On the request of an individual for access to personal information of a medical or psychiatric nature relating to the individual or 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 where 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) must refuse to provide access to personal information pursuant to section 17 (3).

(4) If an organisation is reasonably able to sever information which is referred to in section 17 (2)(b) or section 17 (3)(a), (b) or (c) or 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 must provide the individual with access to the other personal information after the information which is referred to in section 17 (2)(b) or section 17 (3)(a), (b) or (c) or which would be likely to prejudice the physical or mental health of the individual has been severed.

19. Rectification, blocking, erasure and destruction

(1) An individual may request an organisation to correct an error or omission in any personal information about the individual that 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 must, subject to subsection (3):

(a) correct the personal information as soon as reasonably possible, 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) If an organisation declines to make the correction under subsection (2)(a), the organisation must annotate the personal information with the correction that was requested but not made.

(4) On receiving a notification under subsection (2)(b) containing corrected personal information, an organisation must correct the personal information.

(5) Notwithstanding anything in this section, an organisation must not correct or otherwise alter an opinion, including a professional or expert opinion.

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

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

(8) An individual may request an organisation to cease, or not to begin, using personal information about the individual 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 must either cease using the personal information that the individual has identified in their request under subsection (8), or provide the individual with its reasons as to why the use of such personal information is justified.

(10) An individual may request an organisation to erase and/ or destroy personal information about the individual where the use of that personal information is not relevant.

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

20. Procedures for access and correction

(1) For an individual to obtain access to personal information about that individual or make a request for a correction to personal information about that individual, the individual must 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 written request is made.

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

(3) Subject to subsection (4), an organisation must respond to an applicant not later than:

(a) 45 days from the day that 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 (5).

(4) An organisation is not required to comply with subsection (3) during the pendency of 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 sections 17, 18 or 19.

(5) An organisation may, with respect to a request made under sections 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) the applicant does not give enough detail to enable the organisation to identify the personal information,

(b) a large amount of personal information is requested or must be searched or corrected,

(c) meeting the time limit would unreasonably interfere with the operations of the organisation, or

(d) 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.

(6) If the period for responding is extended under subsection (5), the organisation must 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.

(7) An organisation may charge an applicant who makes a request under sections 17, 18 or 19 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.

(8) If an organisation is intending to charge an applicant a fee for a service, the organisation may require the applicant to pay a deposit in the amount determined by the organisation.

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

(10) If an organisation refuses to take action at the request of an applicant, the organisation must inform the applicant of the reasons for the refusal and of the possibility of contacting the Commissioner to make a complaint.

21. Compensation

(1) An individual who suffers damage by reason of any contravention by an organisation of any of the requirements of this Act, is entitled upon application to a court to compensation from the organisation for that damage.

(2) An individual who suffers distress by reason of any contravention by an organisation of any of the requirements of this Act, upon application to a court, is entitled to compensation from the organisation for that distress.

(3) In proceedings brought against an organisation by virtue of this section, it is a defence to prove that it had taken such care in all circumstances as was reasonably required to comply with the requirement concerned.

(4) For the purposes of subsections (1) and (2) above damage means pecuniary or financial loss and distress means emotional disturbance or upset.

(5) The amount of compensation that an individual is entitled to under this section will be limited to [INSERT AMOUNT] for each contravention.

Part 4 – Exemptions

22. National security exemption

(1) 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 purpose of safeguarding national security.

(2) In order to rely on subsection (1) above, organisations must first obtain a certificate signed by the Minister certifying that an exemption from all or any of the provisions of Parts 2 and 3 of this Act is required for the purpose there mentioned.

(3) A certificate under subsection (2) may identify the personal information to which it applies by means of a general description and may be expressed to have prospective effect.

(4) Any person directly affected by the issuing of a certificate under subsection (2) may appeal to the court against the certificate.

(5) If on an appeal under subsection (4), the court finds that, applying the principles applied by the court on an application for judicial review, the Minister did not have reasonable grounds for issuing the certificate, the court may allow the appeal and quash the certificate.

23. Crime and Taxation exemption

Parts 2 and 3 of this Act except for the minimum requirements do not apply to the use of personal information, in any case where such use is required for any of the following purposes:

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders,

(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,

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

(e) important 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 to which the application of those Parts would be likely to prejudice any of the matters mentioned in this section.

24. Regulatory activity and honours exemption

(1) 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 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) for protecting members of the public against-

(i) financial loss due to dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment or other financial services or in the management of bodies corporate,

(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 incompetence of, persons authorised to carry on any profession or other activity,

(b) for protecting charities against misconduct or mismanagement (whether by trustees or other persons) in their administration,

(c) for protecting the property of charities from loss or misapplication,

(d) for the recovery of the property of charities,

(e) for securing the health, safety and welfare of persons at work, or

(f) for protecting persons other than persons at work against risk to health or safety arising out of or in connection with the actions of persons at work.

(3) In subsection (2) "relevant function" means:

(a) any function conferred on any person by or under any enactment,

(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.

25. Further exemptions

The Minister may make regulations setting out further exemptions from Parts 2 and 3 except for the minimum requirements, when such exemptions constitute a necessary and proportionate measure in a democratic society to safeguard an important economic or financial interest of Bermuda including monetary, budgetary and taxation matters.

Part 5 - Supervision

26. Appointment of the Commissioner

(1) For the purposes of this Act there shall be an independent officer known as the Privacy Commissioner.

(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 entry into force of this Act, part of which may take place for a shorter period where the Minister considers a shorter period to be necessary.

(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 authorize 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.

27. Staff

(1) The Commissioner may engage employees to assist in the discharge of his functions.

(2) The Commissioner may, in addition, engage from time to time such technical or professional advisers as the Commissioner 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.

28. Funding for Office and accounting

(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 the Commissioner.

(3) The Commissioner shall cause proper accounts to be kept and maintained of all the financial transactions with respect to the office of the 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 Commissioner shall be audited and reported on annually by the Auditor General, and for that purpose the Auditor General or any person authorized by him shall have access to all books, records, returns and other documents relating to such accounts.

29. General powers of the Commissioner

(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) inform 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 existing or proposed programs of organisations;

(g) 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;

(h) give advice and recommendations of general application to an organisation on matters relating to the rights or obligations of an organisation under this Act;

(i) 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;

(j) make recommendations to the Minister concerning the designation of any jurisdiction as providing a comparable level of protection for the purposes of section 15(2);

(k) make an order at his or her discretion to permit an organisation to transfer personal information to a third party for use either on behalf of the organisation or for that third party's own business practices, where the organisation has reasonably demonstrated that it is unable to comply with section 15(1);

(l) charge such fees as he or she thinks fit for any services provided by him or her under this Act;

(m) do anything which reasonably appears to him or her to be incidental or conducive to the carrying out of his or her 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 honoured;

(c) personal information has been used by an organisation in contravention of this Act or in circumstances that are not in compliance with 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 subject to any fee (not exceeding the prescribed maximum) levied by the Commissioner on the organisation.

(4) When the Commissioner considers that there may have been or there could be a breach of this Act, the Commissioner may serve a person with a notice requiring the person, 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) above, the person shall comply with the requirements in the notice save for communications between the person and his or her 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.

30. Power to authorise an organisation to disregard requests

If an organisation asks, 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.

31. Powers concerning investigations and inquiries

(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 law and the powers given by subsection (2) of this section.

(2) The Commissioner may require any information to be produced to the Commissioner and may examine any 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, an organisation must produce to the Commissioner within 10 days any information or a copy of any information required under subsection (1) or (2), and any applicable legal privilege will not be affected by such disclosure.

(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 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 a review or investigating a complaint, the Commissioner must 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.

32. Guidance and Codes of Practice

(1) The Commissioner may issue guidance from time to time as to compliance with this Act and guidance as to compliance with regulations made under this Act, and shall arrange for appropriate publication of such guidance.

(2) The Minister shall, following consultation with the Commissioner, establish codes of practice providing good practice advice for organisations to comply with the Act.

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

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

(5) 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.

(6) The code of practice is admissible in evidence in any legal proceedings.

(7) 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 the carrying out of those functions, in relation to any time when it was in force, that provision of the code of practice must be taken into account in determining that question.

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

33. Statements not admissible for prosecution

(1) Any written statement provided by a person in response to a notice served on them by the Commissioner under section 29 may not be used in evidence against that person on a prosecution for any offence except –

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

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

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

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

34. Restrictions on disclosure of information

(1) A current or former Commissioner and anyone currently or formerly acting for or under the direction of the Commissioner must not disclose any information obtained in performing their duties, powers and functions under this Act, except as provided in subsections (2) to (5).

(2) A current or former Commissioner may disclose, or the current Commissioner may authorise anyone currently or formerly acting for or under the direction of a Commissioner 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, a current or former Commissioner and anyone acting for or under the direction of the current Commissioner must take every reasonable precaution to avoid disclosing, and must not disclose, any personal information that an organisation would be required or permitted to refuse access to, if access to personal information were requested under sections 17 or 18.

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

(5) A current or former Commissioner may disclose, or the current Commissioner may authorise anyone acting for or under the direction of the Commissioner 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.

35. Protection of the Commissioner and staff

No proceedings lie against a current or former Commissioner, or against anyone acting for or under the direction of a current or 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 Part.

36. Delegation by the Commissioner

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

(2) A delegation under subsection (1) must be in writing and may contain any conditions or restrictions the Commissioner considers appropriate.

37. Reports by the Commissioner

(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 must lay copies of the annual report before each House of the Legislature.

(3) The Commissioner may from time to time, issue reports to the Speaker of the House of Assembly with respect to those functions that the Commissioner thinks fit.

38. Right to ask for a review or initiate a complaint

(1) An individual who makes a request to an organisation respecting personal information about that individual may ask the Commissioner to review any decision, act or failure to act of the organisation.

(2) An individual may initiate a complaint with respect to the issues 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 issues for which a review may be requested or a complaint may be initiated under this Part, the Commissioner may require that an individual asking for a review or initiating a complaint under this Part, must 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.

39. How to ask for a review or initiate a complaint

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

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

(a) 30 days from the day that the individual asking for the review is notified of the decision, or

(b) a longer period allowed by the Commissioner.

(3) A written request to the Commissioner initiating a complaint must 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 when the Commissioner believes the request is without merit or where there is not sufficient evidence to proceed.

40. Notifying others of review or complaint

(1) On receiving a written request for a review, the Commissioner must give a copy of the written request 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 may give a copy of the written request to:

(a) the organisation concerned, and

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

(3) Notwithstanding subsection (1)(a) or (2)(a), the Commissioner may sever 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 person affected by the request.

41. Mediation

The Commissioner may authorise a person to investigate and attempt to mediate and, where possible, to mediate a settlement of any matter under review or relating to a complaint.

42. Inquiry by the Commissioner

(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 a private inquiry to be reasonable.

(3) An individual 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) must 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, must be completed within 180 days from the day that 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 an individual who asks for a review or initiates a complaint or an organisation concerned, the Commissioner must provide reasons for arriving at his or her decisions when conducting an inquiry.

43. Burden of proof

At an inquiry into a decision under which an individual was refused:

(a) access to all or part of the personal information about the individual, or

(b) information concerning the use of personal information about the individual,

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

44. Commissioner's orders

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

(2) If the inquiry relates to a decision of an organisation to give or refuse to give access to all or part of the personal information about the individual, the Commissioner may, by order, do one of the following:

(a) direct the organisation to give the individual access to all or part of the personal information about the individual 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) either 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;

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

(3) If the inquiry relates to any matter other than a matter referred to in subsection (2), 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 honoured or require that a right set out in this Act be honoured;

(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 or in circumstances that are not in compliance with this Act;

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

(f) require an organisation to destroy personal information used in contravention of this Act or in circumstances that are not in compliance with this Act;

(g) require an organisation to provide specific information to individuals in the event of a breach of section 14 (2) which is likely to cause significant harm to individuals.

(4) In the event that an order under section 44 (2) or (3) would not be applicable, then the Commissioner may make such order as the Commissioner 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 must give a copy of an order made under this section to all of the following:

(a) the individual 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;

(d) the Minister.

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

45. No appeal to the Commissioner

Subject to section 46, an order made by the Commissioner under this Act is binding on all persons affected by it and there is no right of appeal to the Commissioner. Upon the order being filed with the Registrar of the Supreme Court, it shall have the effect of an order of the Supreme Court and shall be enforceable in the same manner as an order of the court.

46. Judicial Appeal

(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 must comply with the order.

(2) An organisation must not take any steps to comply with a Commissioner's order until the period for bringing an application for judicial appeal under subsection (3) ends.

(3) Any person aggrieved by an order of the Commissioner under this Act may apply to the Supreme Court for judicial appeal of the order and the application must be made not

later than 45 days from the day that the person making the application is given a copy of the order. The Court, after considering the application, may confirm, vary, remit or set aside the decision.

(4) If an application for judicial appeal is made pursuant to subsection (3), the Commissioner's order is stayed until the application is dealt with by the court.

(5) Notwithstanding subsection (3), 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

47. Disclosure regarding Business Transactions

(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 anything in this Act other than this section, 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 individuals without the consent of the individuals provided that all the following conditions are satisfied, namely -

(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 individuals without the consent of the individuals 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 the individuals, 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 must, 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 that 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 an individual to the use of personal information about the individual for purposes that are 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.

48. Offences and Penalties

(1) Subject to subsections (3) and (4), a person commits an offence if the person:

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

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

(h) knowingly or recklessly fails to comply with section 34 (1);

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

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

(k) contravenes section 7.

(2) A person who commits an offence under subsection (1) is liable,

(a) in the case of an individual, to a fine of not more than [*INSERT AMOUNT*], and

(b) in the case of a person other than an individual, to a fine of not more than [*INSERT AMOUNT*].

(3) Neither an organisation nor an individual is guilty of an offence under this Act, if it is established 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.

(4) 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.

(5) 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 or she, as well as the body corporate, commit that offence and are liable to be proceeded against and punished accordingly.

(6) Where the affairs of a body corporate are managed by its members, subsection (5) applies, in relation to the acts and defaults of a member in connection with his functions of management, as if he or she were a director of the body corporate.

49. Power to make regulations

(1) Subject to subsection (2), at the request of the Commissioner or otherwise but always in consultation with the Commissioner, the Minister may make regulations prescribing all matters under this Act.

(2) The Minister shall not make regulations unless it considers such regulations to safeguard the interests or the rights and freedoms of individuals.

50. Review of the Act

(1) The Minister must carry out a comprehensive review of this Act within 5 years of its coming into force, and must submit a report to the House of Assembly within 18 months after beginning the review.

(2) A report submitted under subsection (1) may include any amendments to this Act or any other Act that are recommended by the Minister.

51. Commencement

(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 the operation of different provisions of the Act.

GOVERNMENT OF BERMUDA
The Ministry of Economic Development
The Department of E-Commerce