FACT SHEET | FREQUENTLY ASKED QUESTIONS

# Personal Information Protection Act

## 1. What is PIPA?

PIPA is the Personal Information Protection Act 2016 ("**PIPA**") which was introduced to regulate the use of personal information in a manner that both protects privacy and recognizes the need for organisations to use personal information for legitimate purposes. PIPA received royal assent in July 2016 though only limited provisions relating to the appointment of the Privacy Commissioner (the "**Commissioner**") and establishment of his office have been operative to date. We expect PIPA to take full effect by the end of 2021.

## 2. Who is affected?

PIPA applies to every organisation in Bermuda that uses personal information where it is used wholly or partly by automated means and in respect of uses other than by automated means of personal information which form, or are intended to form, part of a structured filing system.

"Organisation" is broadly defined as "any individual, entity or public authority that uses personal information" and the "use" of personal information is defined as "carrying out any operation on personal information, including collecting, obtaining, recording, holding, storing, organisation, adapting, altering, retrieving, transferring, consulting, disclosing, disseminating, or otherwise making available, combining, blocking, erasing or destroying it." There is no scope to contract out of PIPA and PIPA provides for the grandfathering of personal information held prior to PIPA coming into effect.

Personal information collected and under an organisation's control prior to PIPA becoming operative, is deemed to have been collected pursuant to consent by the relevant individual and may continue to be used by the organisation for the purpose for which it was collected, at the time it was collected.

## 3. What is considered "personal information"?

PIPA makes a distinction between personal information and sensitive personal information. 'Personal information' is defined quite broadly as being any information about an identified or identifiable individual and consequently, the obligations that PIPA places on organisations, is very wide. 'Sensitive personal information' relates to 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.

## 4. What are the principles of PIPA?

PIPA applies principles and rules for the way personal information must be treated. Personal information must be used fairly and lawfully and be used for a specific limited purpose. Personal information must be accurate, adequate, relevant and not excessive in relation to the intended purpose for which the personal information is obtained and every organisation must protect the personal information that it holds with appropriate and proportionate safeguards against risk, including loss, unauthorised access, destruction, misuse, modification or disclosure.

PIPA also empowers individuals to have more control over their personal information; individuals may request access to their personal information and organisations must provide that individual with access to that individual's personal information in the custody or control of the organisation, the purpose for which the personal information has been and is being used by the organisation, and the names of the personas or types of persons to whom and circumstances in which the personal information has been and is being disclosed.

An individual also has the right to rectify, block, erase and destroy their personal information that is held by an organization where that personal information is no longer relevant for the purposes of its use and may request an organisation cease or not use their personal information for the purposes of advertising, marketing or public relations..

## 5. How does my organisation become compliant with PIPA?

There are key obligations that must be met by organisations that are using personal information to ensure that they are compliant, which, amongst other things, include:

### Policies and Procedures

Every organisation must adopt suitable measures and policies to give effect to its obligations and to the rights of individuals. The policies and procedures must take into account the nature, scope, context and purposes of the use of personal information and the risk to individuals by the use of personal information. An organisation must be mindful when designing policies and procedures that the policies and procedures take into account the general principles and rights of the individual provided for under PIPA.

### Appointment of a Privacy Officer

Every organisation must designate a privacy officer who will have the primary responsibility for communicating with the Privacy Commissioner. 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. While other individuals in an organisation may be involved in handling personal information, the privacy officer for each organisation will also be accountable for structuring, designing and managing the privacy management program of an organisation, which will include any policies, practices, training, internal audit and evaluation.

### Privacy Notices

Every organisation must provide individuals with a clear and easily accessible privacy statement about its practices and policies with respect to personal information. The privacy statement must include certain information, such as, amongst others, the fact that personal information is being used, the identity and types of individuals or organisations to whom personal information might be disclosed and the name of the privacy officer.

### Obtaining Consent for the 'Use' of Personal Information

As a general rule, organisations may only use personal information with the consent of the individual where the organisation can reasonably demonstrate that the individual has knowingly consented. In the absence of consent, the circumstances under which organisations are allowed to use personal information are limited. Consent provides individuals with control over how their personal information will be collected, used and disclosed. An organisation is not obliged to provide a mechanism for consent, such as a privacy notice, where it can be reasonably implied from the conduct of an individual that the individual consents to the use of personal information for all intended purposes, however this does not apply to sensitive personal information. Where an individual consents to the disclosure of their 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. Additionally, an individual will be deemed to have consented to the use of their 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 benefit from such a plan.

## 6. Can an organization outsource its responsibilities under PIPA?

PIPA establishes that 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 the legislation at all times. A 'third party' is not defined in PIPA.

## 7. Are there different obligations for using sensitive personal information?

Sensitive personal information can only be used with lawful authority if and only to the extent that it is used: with the consent of any individual to whom the information relates; in accordance with an order made by either a court or the Privacy Commissioner; for the purposes of criminal or civil proceedings; or in the context of recruitment or employment where the nature of the role justifies such use.

## 8. Are there special measures for personal information relating to children?

Where an organisation uses personal information about a child in the provision of an information society service and the service is targeted at children or the organisation has actual knowledge that it is using personal information about children, the organisation must obtain consent from a parent or guardian before the personal information is collected or otherwise used. An organisation delivering an information society to a child shall provide a privacy notice that is compliant in accordance with PIPA that is easily understandable and appropriate to the age of the child.

PIPA defines 'information society' as a service which is delivered by means or digital or electronic communications and a 'child' means an individual under the age of 14.

## 9. Are there restrictions on transferring information to an overseas third party?

When an organisation transfers 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 purpose, the organisation remains responsible for compliance with PIPA in relation to the personal information. Before making any such transfer, the organisation must assess the level of protection provided by the overseas third party for the personal information. If an organisation reasonably believes that the protection provided by the overseas third party is comparable to the level of protection required by PIPA, as evidenced by the third party's adoption of a certification mechanism recognised by the Commissioner, the organisation may rely on that level of protection while the personal information is being used by the overseas third party.

The Commissioner currently recognises the Asia Pacific Economic Cooperation ("APEC") Cross Border Privacy Rules ("CBPR") System as a certification mechanism for the transfer of personal information to an overseas third party.

If an overseas third party claims to be CBPR-certified, organisations should verify their claim by consulting the public Compliance Directory available at http://cbprs.org/. and should ensure that CBPR certification is a material part of their agreement with the overseas third party.

Even if relying on an overseas third party's CBPR certification, organisations remain responsible to the individual and must provide appropriate notice (including notice regarding the transfer overseas and its reliance on a particular certification mechanism) and fulfil any other responsibilities under PIPA.

## 10. What are the consequences for non-compliance?

An individual who suffers financial loss or emotional distress through an organisation's failure to comply with its requirements under PIPA is entitled to compensation from the organisation.

The Commissioner can make orders, issue formal warnings and make public admonishments in respect of a non-compliant organisation. Further, a person or organization who commits an offence under PIPA may be liable on summary conviction in the case of an individual, to a fine of up to $25,000 and up to two years imprisonment and in the case of conviction of an entity on indictment, to a fine not exceeding $250,000.