

## Is your organisation PIPA ready?

Service area / [Employment, Pensions and Incentives](#)

Legal jurisdiction / [Bermuda](#)

Date / [January 2023](#)

Bermuda's Privacy Commissioner has recently announced that the island's first data privacy legislation, the Personal Information Protection Act 2016 (PIPA), may soon be coming into effect, at least for some businesses.

This briefing sets out the key requirements of PIPA and the steps that your organisation can take to prepare for its implementation.

### PIPA coming into force

PIPA was enacted in 2016 to regulate the use of personal information in Bermuda by individuals, companies, public authorities and other organisations. Although some of PIPA's provisions came into effect shortly after enactment, including those which established Bermuda's Privacy Commissioner, PIPA's operative provisions, which set out the responsibilities of data users and the specific rights of data subjects, have yet to come into force.

It has recently been reported that the government now aims to bring PIPA's main provisions into effect from Spring 2023. The Privacy Commissioner has stated that these provisions could be implemented in phases, with certain rules enforced for some organisations before others. The Privacy Commissioner has suggested, for example, that exempt undertakings, which may already comply with data protection regimes in other jurisdictions due to the international nature of their businesses, could be the first organisations required to comply with PIPA.

The Privacy Commissioner has also confirmed that his office plans to publish guidance, including checklists and templates, to assist organisations prepare for PIPA compliance. Notably, the Commissioner's office has received funding to double its headcount this year.

This long-anticipated implementation of PIPA's key provisions would set the scene for Bermuda's hosting of the 2023 Global Privacy Assembly in October, an event which could bring hundreds of international privacy officers and technology executives to the island.

### Preparing your organisation for PIPA

Under PIPA, your organisation will need to adopt suitable measures and policies to give effect to its obligations and the rights of individuals. These measures and policies should be reasonable, taking into account the nature, scope, context and purposes of the use of personal information as well as the potential risk to individuals due to the use of their personal information.

As we set out below, there are various steps that your organisation can take in anticipation of PIPA's enforcement.

#### Determine whether your organisation is already PIPA compliant

Organisations which are compliant with international privacy regimes may already have policies in place which fulfil PIPA requirements. For example, the EU's General Data Protection Regulation and PIPA are based on similar principles.

It may be prudent to seek legal advice to determine the extent to which your organisation is already compliant with PIPA.

#### Determine the legal basis for your organisation's use of personal information

For the purposes of PIPA, 'personal information' includes any information about an identified or identifiable natural person.

### OFFSHORE LAW SPECIALISTS

BERMUDA BRITISH VIRGIN ISLANDS CAYMAN ISLANDS GUERNSEY JERSEY  
CAPE TOWN HONG KONG SAR LONDON SINGAPORE

Some personal data is excepted from PIPA requirements, including business contact information used to contact an individual in their capacity as an employee or official of an organisation, and personal information about an individual who has been dead for at least 20 years.

Stricter rules apply to the category of 'sensitive personal information', which includes data about an individual's race, sexual orientation, religious belief, political opinion, disability and medical information.

Under PIPA, your organisation may only use personal information where there is a lawful basis for that use. Such lawful bases include:

- when the organisation has the knowing consent of the individual to that use;
- where the individual would not reasonably be expected to object to that use (except in relation to sensitive personal information);
- where using that information is necessary for the performance of a contract to which the individual is a party;
- where the use is authorised or required by law; and
- where the use is necessary in the context of an individual's employment relationship with the organisation.

PIPA also specifies circumstances in which an individual may be deemed to have given their consent to the use of their information, including where consent can be reasonably implied from the individual's conduct, or where the information is used for the purpose of coverage or enrolment under an insurance, trust, benefit or similar plan.

### Ensure all personal information is relevant

Your organisation must ensure that all personal information it holds is accurate, up to date, adequate, relevant, and proportionate to the purposes for which it is to be used. Personal information must also only be kept as long as is necessary for its use.

### Ensure all personal information is secure

Your organisation will need to implement safeguards to protect personal information against risks of unauthorised access, destruction, use, modification or disclosure. These safeguards must be proportional to the likelihood and severity of harm, the sensitivity of the personal information, and the context in which the information is held.

### Prepare terms to govern transfers to third parties

Where your organisation transfers personal information to an overseas third party, your organisation will remain responsible for PIPA compliance in relation to that personal information.

If your organisation does not believe that the protection provided by the overseas third party will be comparable to that required by PIPA, your organisation may choose to employ contractual mechanisms, corporate codes of conduct, or other means to ensure that adequate protection is provided.

### Appoint a privacy officer

Your organisation will need to designate a 'privacy officer', who will have primary responsibility for communicating with the Privacy Commissioner. The privacy officer may also be the main point of contact for individuals who wish to inquire about your organisation's use of their personal information.

It is possible for a group of organisations under common ownership or control to appoint a single privacy officer.

### Prepare privacy notices

PIPA also required that an organisation take reasonably practical steps to provide a 'privacy notice' to each individual before or at the time their personal information is collected.

A privacy notice should be clear and easily accessible, and must provide the individual with details of the organisation's practices and policies in relation to personal information, including:

- the purpose(s) for which their personal information is or might be used;
- the identity and types of third parties to whom their personal information might be disclosed;
- the identity, location and contact details of the organisation;
- the name of the organisation's privacy officer; and
- the choices and means the organisation provides to the individual to access, rectify, block and/or destroy their personal information.

Generally, an organisation may only use personal information for the purposes set out in the privacy notice.

### Familiarise yourself with individuals' rights under PIPA

Although it is expected that the relevant sections of PIPA may be the last to come into force, it is nonetheless worth familiarising yourself with the rights of individual data subjects, which include:

- the right to access the personal information which an organisation holds about them;
- the right to request that an organisation corrects errors or omissions in their personal information;
- the right to demand that an organisation not use their personal information for marketing; and
- the right to demand that an organisation erase or destroy personal information which is no longer relevant.

### Get in touch

If you would like to discuss how PIPA might impact your organisation, please contact the Carey Olsen team.

Continued



---

## FIND US

Carey Olsen Bermuda Limited  
Rosebank Centre 5th Floor  
11 Bermudiana Road  
Pembroke HM 08  
Bermuda

T +1 441 542 4500

E [bermuda@careyolsen.com](mailto:bermuda@careyolsen.com)



---

## FOLLOW US

Visit our employment, pensions  
and incentives team at  
[careyolsen.com](http://careyolsen.com)



---

## PLEASE NOTE

Carey Olsen Bermuda Limited is a company limited by shares incorporated in Bermuda and approved and recognised under the Bermuda Bar (Professional Companies) Rules 2009. The use of the title "Partner" is merely to denote seniority. Services are provided on the basis of our current terms of business, which can be viewed at: [www.careyolsen.com/terms-business](http://www.careyolsen.com/terms-business).

This briefing is only intended to provide a very general overview of the matters to which it relates. It is not intended as legal advice and should not be relied on as such. © Carey Olsen Bermuda Limited 2023.