CAREY OLSEN

Is your organisation PIPA ready?

Service area / Regulatory compliance
Legal jurisdiction / Bermuda
Date / August 2024

The operative provisions of Bermuda's first data privacy legislation, the Personal Information Protection Act 2016 (**PIPA**), will come into effect from 1 January 2025. PIPA will regulate the use of personal information by 'organisations' in Bermuda, which under the legislation will include individuals, companies, public authorities, and other entities.

This briefing sets out the steps that your organisation can begin to take now to prepare for its coming obligations under PIPA.

PIPA provisions currently in force

When PIPA was enacted in 2016, a limited number of its provisions were brought into force with immediate effect, including provisions establishing the office of Bermuda's Privacy Commissioner.

The Privacy Commissioner has been responsible for developing and maintaining Bermuda's data privacy regime. So far, this has included issuing guidance and recommendations in relation to the implementation of PIPA, advising on policies and legislation which may affect privacy, and educating the public on privacy-related issues. Going forward, the Commissioner will also oversee organisations' compliance with PIPA, including receiving and investigating complaints, reviewing reports of security breaches, and ordering organisations to take specific actions to comply with the legislation.

Your organisation may find the Commissioner's published guidance to be a useful resource. It can be found on the Commissioner's website here.

Preparing for 2025

From 1 January 2025, your organisation will need to adopt reasonable measures and policies to ensure its lawful use of personal information. Below, we set out suggested steps that your organisation should take now in the lead up to PIPA's enforcement, and which can form part of a more focused plan to prepare for compliance.

Determine whether your organisation is already PIPA compliant

Organisations that are subject to international privacy regimes may already have policies in place which will fulfil some of their obligations under PIPA. For example, organisations which are compliant with the EU's General Data Protection Regulation (**GDPR**) will likely already have policies and procedures in place and be capable of responding to data subject access requests.

Nevertheless, the Privacy Commissioner recommends that all organisations, including those that are GDPR compliant, reevaluate and update their privacy policies and procedures to ensure specific compliance with PIPA.

Determine what personal information your organisation uses

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

Some personal information is categorised as 'sensitive' and is subject to stricter rules in relation to its use. Sensitive personal information includes, but isn't limited to, information in relation

to: race, national or ethnic origin, sex, sexual orientation, disability, physical or mental health, family status, religious beliefs, political opinions, and biometric information (e.g. fingerprints).

'Use' is defined broadly by PIPA as the carrying out of any operation on personal information. This includes, but is not limited to, collecting, holding, consulting, altering, organising, transferring, and destroying it.

PIPA will require your organisation to ensure that all the personal information you hold is accurate, proportionate to the purposes for which it is held, and not kept any longer than is necessary to fulfil those purposes.

The first step towards compliance is for your organisation to complete an in-depth investigation to identify the extent of the personal information it currently uses, and the purposes for which it is used.

Determine the legal bases for your organisation's uses of personal information

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

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

PIPA specifies some circumstances in which an individual may be deemed to have consented to the use of their personal information, including where such information was collected by an organisation prior to 1 January 2025 (provided the organisation only uses the information for the purposes for which it was collected).

Familiarise yourself with individuals' rights in relation to their information

Your organisation should familiarise itself with the rights that individuals will have in relation to your organisation's uses of their personal information, including:

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

Ensure all personal information held 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.

Your organisation should conduct a risk assessment exercise to determine what safeguards should be implemented.

Determine whether personal information is transferred to third parties

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

Where an organisation transfers information to a third party located overseas, it must assess whether the protection provided by that third party will be comparable to that required by PIPA. The organisation may choose to employ contractual mechanisms, corporate codes of conduct, or other means to ensure that adequate protection is provided.

Your organisation should determine the circumstances in which it might transfer personal information to third parties, the protections offered by those parties, and the extent to which your organisation should supplement those protections.

Appoint a privacy officer

Your organisation will need to designate a 'privacy officer', who will be responsible for communicating with the Commissioner and will be the main point of contact for individuals who wish to inquire about your organisation's use of their personal information.

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

Prepare privacy notices

PIPA will require that organisations 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 purposes 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.

Continued

How we can help

PIPA takes a proportionate approach in relation to the measures organisations will be required to implement to achieve compliance with the legislation, specifying that, in meeting their responsibilities under PIPA, organisations must 'act in a reasonable manner'. Notwithstanding this, for many organisations, PIPA will require significant planning and groundwork.

Please contact our team to discuss how Carey Olsen can assist your organisation to prepare for PIPA, including by:

- providing training to your board and/or staff;
- assisting with your due diligence and risk assessment exercises;
- providing template/bespoke policy documents, privacy notices and framework; and
- drafting contractual terms in relation to transfers of information to third parties.

Subscribe for more

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

FOLLOW US

Subscribe for more

Visit our regulatory team at careyolsen.com

PLEASE NOTE