Article

Understanding PIPA: Defining its Scope and Starting to Prepare

Authors: Julie McLean, Director | **Andrew Barnes,** Associate | **Sarah Blair,** Associate

In a four-part series, Conyers will be diving into different topics relating to Bermuda's privacy legislation, including: why we need privacy legislation and its purpose, how do we prepare for PIPA, the role and requirements of privacy officers, and what are our rights as individuals? In this second part, Conyers discusses to whom PIPA applies and what organisations can do to prepare for its implementation.

In the first part of this series we discussed why data and privacy legislation has developed and its purpose. We also provided a brief introduction to Bermuda's privacy legislation, the Personal Information Protection Act 2016 ("PIPA"). While the substantive provisions of PIPA have not yet come into force, and we do not yet have a date for implementation, many organisations have already begun the process of getting "PIPA-prepared". Indeed, the Privacy Commissioner and his team have been providing helpful community outreach and guidance to assist with this process. However, it understandably remains a challenge to know where to begin.

Before being able to establish any privacy program, an organisation needs to first understand whether PIPA applies to it and what personal information it is holding or has control over. Essentially they need to conduct an "information inventory". This is not as scary as it sounds but does require management to consider a number of factors.

To whom does PIPA apply?

PIPA applies to all *organisations* – being any individual, entity (e.g. companies, associations, non-profits and charities) or public authority that:

(i) *uses personal information in Bermuda* (PIPA does not apply to the use of personal information outside of Bermuda); and

(ii) where that personal information is used wholly or partly by *automated means* (electronically in computer files) or where its use, if not by automated means, forms (or is intended to form) *part of a structured filing system*.

While we delve further into these aspects further below, it should be noted that PIPA does include certain practical exclusions. PIPA does not apply, for example, to the use of personal information for: (i) personal or domestic purposes (for example, a guest list for a party); (ii) artistic, literary or journalistic purposes with a view to publication in the public interest where seen as necessary to protect the right to freedom of expression; or (iii) the use of business contact information for purposes of contacting an individual in their capacity as an employee or official of organisation (e.g. a law firm can list its lawyers and their business contact information on the firm's website).

Where is the personal information being used?

PIPA is only applicable to personal information that is being used *in Bermuda*. For local organisations, PIPA will therefore likely be applicable. However, an example where it might not be applicable is if an exempt company has a US office where all the human resource functions are undertaken with no records being kept, used or obtainable in Bermuda. In such a case, the personal information held and used by the US office is not caught by PIPA.

What personal information is being collected and used by the organisation?

PIPA concerns the use of personal and sensitive personal information. We covered the definitions of these terms in the first article of our series. In brief, 'personal information' is broadly defined and means "any information about an identified or identifiable individual" (i.e. a natural person whether they are explicitly identified by name or where their identity is identifiable from a piece of information, such as their social insurance number). 'Sensitive personal information' refers to certain and, more sensitive, data about an individual, for example their place of origin, race or sexuality.

An organisation needs to understand what information it is collecting and using to know if they are caught by PIPA. For example, retail companies often ask for telephone numbers and emails from their customers. Doctors and dentists collect the personal and sensitive personal information necessary to provide the appropriate care to their patients. Insurance companies will collect personal and sensitive personal information in order to provide life insurance or medical coverage. In addition to considering what personal information they collect from customers, an organisation should also identify what personal information it is collecting from its employees.

How is the personal information being stored?

As set out above, PIPA applies to personal information being used wholly or in part by automated means or, if not by automated means, where it forms, or is intended to form, part of a structured filing system.

By way of example, if a restaurant takes a person's name and telephone number for a take-out order but then throws away the order form once the food is collected, such information is arguably not part of a structured filing system and the organisation is not caught under PIPA (in respect of this personal information at least). However, if the restaurant stores the customer's information in a Filofax for future reference, or has an online ordering system where the customer's details are stored electronically, then the personal information would be subject to PIPA.

What is the purpose of collecting the personal information?

Pursuant to PIPA, once implemented, the information being collected should only be used for the specific purpose for which it's collected and for which the individual would reasonably expect it to be used. An organisation should therefore consider its purposes for collecting information and whether or not these fall within the permitted categories in PIPA or if they need to obtain further consents. For example, a dentist office will collect personal information on a patient to be able to provide the required dental care. However, if it uses the personal information to send a birthday email to the patient, that is arguably using the personal information for the purpose of business promotion or marketing and the patient's consent should be obtained for using it in this way before doing so. Organisations need to have a clear understanding as to why they are collecting the personal information so they can ensure it is used only for that purpose. In addition, it is important that the organisation is transparent about the use of such personal information and makes the purpose clear in their privacy notice.

Where is the information stored?

This may be a difficult question for an organisation to address and it may require the assistance of their technology team. It's important to know where the personal information is stored as the individual has certain rights under PIPA which the organisation can only address properly if it knows where all the personal information stored on that individual is kept. An organisation may have physical hard copies kept in a filing cabinet or vault. In addition, it may have an electronic database where the personal information on clients and employees is stored. The personal information may have been submitted by email so it is also stored in the email filing system. Another aspect to this question is whether such information is only stored in Bermuda or has the organisation transferred it somewhere else for storage? PIPA imposes specific obligations on organisations who transfer personal information to overseas third parties.

How old is the personal information in the organisation's control?

You may remember from our first article that one of the underlying principles of PIPA is that personal information should not be kept any longer than is necessary for its use. For example, if a real estate company has requested personal information on a buyer of a property in order to satisfy anti-money laundering rules, they need to consider how long they are required to keep such information on file to satisfy the anti-money laundering legislation. Once it's no longer needed, they should consider having a procedure in place to delete such information from their records.

Going through the questions above will hopefully help an organisation with their preparations for PIPA. Once an organisation has clarified that PIPA applies to them, it will need to appoint a privacy officer, implement an appropriate privacy programme and ensure its staff are trained. Some organisations may prefer to appoint a privacy officer first who will then be tasked with carrying out the information inventory. The next part in this Conyers PIPA series will address the role and responsibilities of the privacy officer.

Disclaimer: Nothing in this article constitutes legal advice and is for general purposes only. If you would like to obtain legal advice on PIPA, please contact the Conyers team:

Authors:

Julie McLean
Director
julie.mclean@conyers.com
+1 441 299 4925

Andrew Barnes
Associate
andrew.barnes@conyers.com
+ 1 441 278 8054

Sarah Blair
Associate
sarah.blair@conyers.com
+ 1 441 279 5335