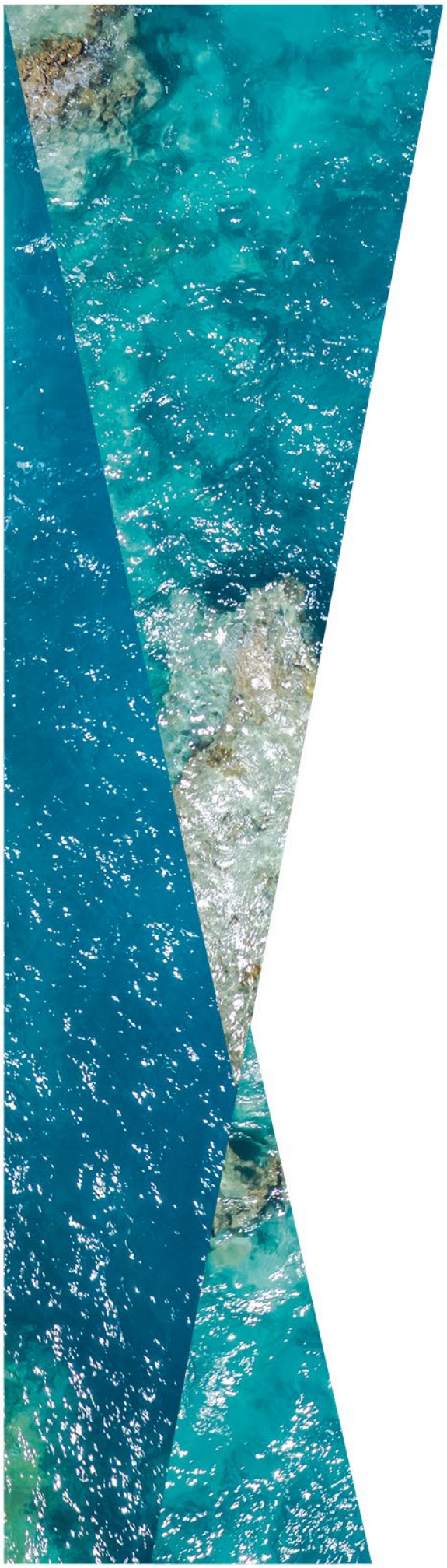


PIPA Is Fully in Force – Now What?

Practical insights for Bermuda organisations grappling with the now fully in force Personal Information Protection Act 2016

21 January 2025

ATTORNEY CONTRIBUTOR

Ms. Gretchen Tucker is Counsel, Head of Regulatory & Governance at BeesMont Law Limited.

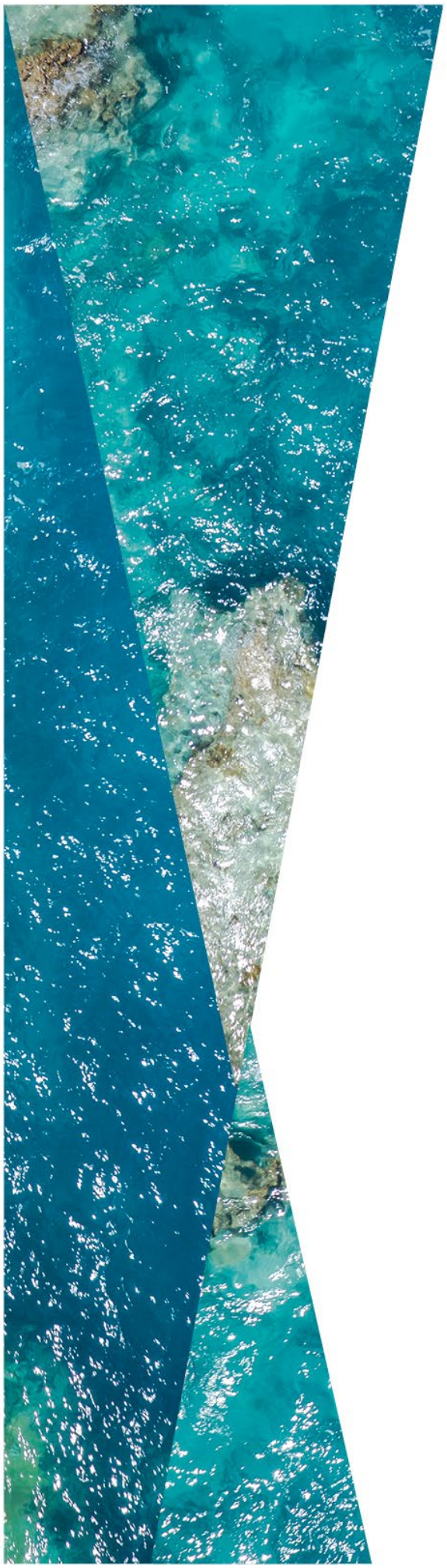
As a dual-qualified barrister, her practice encompasses regulatory compliance, administrative decision-making, statutory interpretation, policy development and legal reform which extends to advising on privacy, access to information as well as the use of employee and children's data and health sector information.

On 1 January 2025, the Personal Information Protection Act 2016 (**PIPA**) came fully into force in Bermuda. Applauded by the international and local data protection communities alike, PIPA is intended to create a balance between the need to protect the informational privacy rights of the individual and the need for organisations to use their personal information for appropriate purposes.

PIPA is not the "equivalent" of the data protection frameworks of the European Union (**EU**) or the United Kingdom (**UK**) and does not adopt the concepts of "controller" & "processor". Notably, there is no statutory right to use personal information for a "legitimate interest" purpose. PIPA, however, is not intended to operate in isolation from global data protection frameworks and adopts privacy standards from the EU, Canada and the Cayman Islands. These standards have been "Bermudianised" to provide a lighter regulatory approach by reducing some of the traditional regulatory requirements found in these jurisdictions to provide more operational flexibility for organisations.

PIPA Is Fully in Force – Now What?

Notwithstanding this strategic drafting approach, in the absence of Bermuda organisations being subject to any over-arching data protection framework for decades (and only constitutional, common law and sectoral laws), grappling with PIPA can be a daunting prospect. Regardless of size and resources, it may be tempting for many Bermuda organisations to simply appoint an existing staff member as the privacy officer, publish a generic privacy notice and plan to complete a review of data usage and prepare a breach notification response at a later date. Indeed, this will be the approach for many internal teams in Bermuda feeling overwhelmed by the new requirements and anxious to appear to be doing "something" in



response to these regulatory developments. To do so, however, could create a false expectation that your organisation has a clear understanding of data flows as well as having adequate controls and measures to protect the personal information it holds. In the long term, such hasty practices may not only fall afoul of PIPA but also give rise to new causes of action, reduce customer trust and result in damage to brand reputation and profit. We have already seen this occur in the United Kingdom and other jurisdictions where over-arching data frameworks have been introduced and Bermuda organisations would be wise to avoid the same pitfalls.

There is also the possibility that a substantive aspect of an organisation/s use of personal information actually falls outside the regulatory scope of PIPA. It would be unfortunate to (belatedly) discover that market conduct in 2025 created a legal obligation which did not already exist under PIPA.

Investing in Organisational Oversight

Accountability is a vital aspect of any successful privacy programme. Ensure that your internal teams are well-positioned to, collectively, advance PIPA risk management & compliance initiatives:

- **Prioritise education at the top level.** If your organisation is behind on PIPA preparedness (or if internal efforts appear to be somewhat unprogressive), the underlying issue may be a lack of understanding of the key statutory requirements. If your Board and Executive Team do not understand PIPA, they will not be properly positioned to consider and approve segments of your organisation's privacy programme (although they may be potentially liable to statutory enforcement action in the event that the organisation is found to be non-compliant). Schedule time to meet and conduct the following review of PIPA:

  Do any exclusions or exemptions apply to our organisation?

  - Section 4 – read and identify whether any of your organisation's use of personal information falls within a category excluded from the scope of PIPA.
  - Sections 22-25 – read and identify whether any of your organisation's use of personal information falls within the scope of an exemption (which could reduce the extent to which your organisation would need to comply with PIPA).

  What are our organisation's over-arching responsibilities and which appointees can be penalised?

  - Section 5 – read and identify the limited statutory responsibilities of the privacy officer.
  - Section 14 – read and identify what triggers a reporting obligation to Privacy Commissioner.
  - Section 47 – read and identify penalties for corporate bodies, directors, managers and secretaries. Note that the privacy officer is not expressly identified, which underscores that the ultimate responsibility rests with the management of the organisation.

  Are we using sensitive personal information and what security safeguards are appropriate?

  - Section 7 – read and identify scenarios where your organisation is using sensitive personal information.
  - Section 13 – read and identify current security measures and whether they are heightened when sensitive personal

information is involved.

How can we lawfully continue to use personal information?

- Section 6 – read and identify which conditions can be relied upon for continued use of personal information in the context of your workforce, client relationships, vendor relationships and visitors to your website. Identify current marketing practices and whether these would fall afoul of PIPA without any changes being made to the same.

What information needs to go into our privacy notices?

- Section 9 – read and consider strategies to provide the privacy notice to the individual before or at the time of collection of personal information.

What is the statutory process for individuals to make requests to organisations or access, correction, block, erase or destroy their personal information?

- Section 19 – read and consider strategies to ensure organisations can adhere to prescribed statutory timeframes for responses.

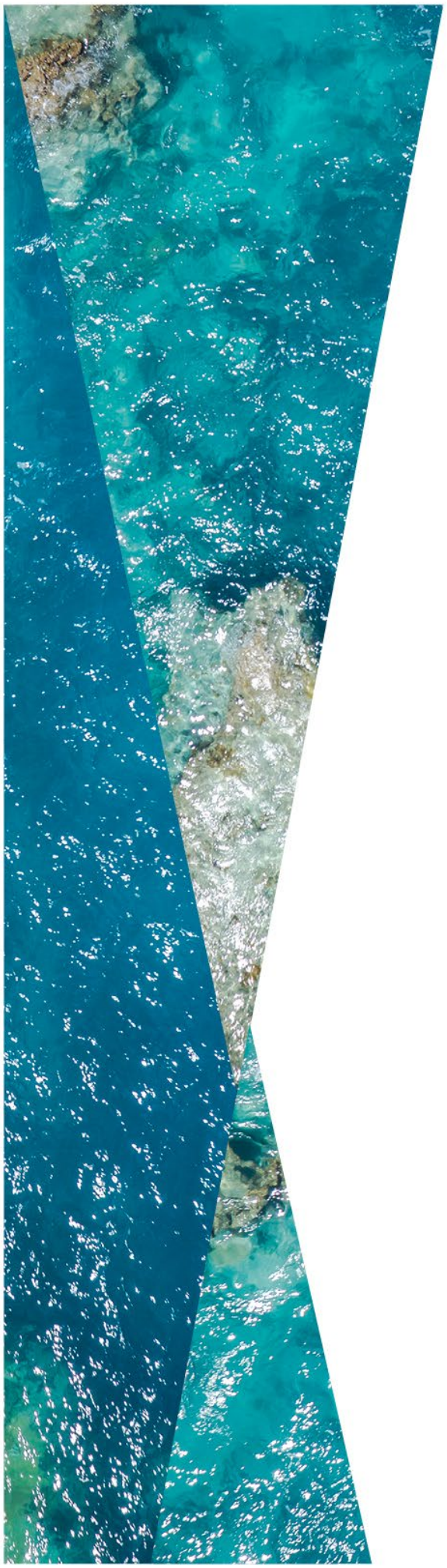
- **Create a privacy committee.** PIPA does not establish that the statutory Privacy Officer role is responsible for the creation and deliver of an organisation's privacy programme. This is for good reason as it is ultimately the Board and Executive Team which establish any business strategy to be adopted by the enterprise, and personal information is typically used to achieve the same. Moreover, it is the Board and the Executive Team which must be responsive to both stakeholder and shareholder concerns as well as regulatory and industry trends in the market (i.e. establishment of ESG and DEI programmes). Ideally, organisations should establish a privacy committee which includes members from all divisions involved in critical decision-making roles (Board, Executive, HR, IT, Administrative) in addition to the Privacy Officer. Notably, the majority of these roles will have pre-existing knowledge of the organisation's use of personal information.

- **Don't rely on generic privacy notices.** Template privacy notices with boilerplate language often reference foreign law concepts such as "legitimate interests", "controller" and "processor" which are not adopted by PIPA. Reliance on such language in templates (including internal templates in the case of multi-national organisations with Bermuda-based offices) can cause your organisation to breach Bermuda law requirements and create confusion for the data subject.

- **Don't bundle *all* use cases into a single privacy notice.** PIPA requires privacy notices to be clear and easily accessible. Referencing all use cases into one notice often creates a document that is as clear as mud and can cause your organisation to breach Bermuda law requirements. Instead, opt to create a series of privacy notices. Use of personal information by an organisation is typically contextual. The starting point for any privacy notice should be the relationship with the individual. Consider creating privacy notices responsive to:
  - the workforce (including temporary workers and students);
  - client relationships;
  - third party relationships (donors, vendors, investors); and
  - website visitors.

- **Do adopt a "less is more" approach.** Don't know what to say in a privacy notice? Start with the listing set out in Section 9 of PIPA which confirms what organisations must communicate to individuals. Build out the language based on what you know about the current status of your organisation's use of personal information.
- **Do identify where knowledge gaps exist within your organisation and how best to close the same**. Mostly commonly discussed solutions in this respect include training initiatives, direct hires as well as obtaining support from Bermuda counsel and other third party service providers and advisors. These steps can support the achievement of specific privacy-oriented goals. However, they may not reveal all gaps in an organisation's enterprise risk management (**ERM**) programme. For these reasons, organisations should also consider adopting tabletop exercises to respond to threat scenarios involving personal information. For example, how would an organisation respond to a cybersecurity event which triggers a reporting obligation to the Privacy Commissioner:
    - What is the existing emergency response protocol and recovery plan?
    - What information needs to be communicated to the Privacy Commissioner? What information needs to be communicated to the data subjects affected? Are there any relevant deadlines to consider?
    - For organisations which are conducting business pursuant to a licence, is there a secondary reporting obligation and what information needs to be communicated? Is there a relevant deadline?
    - In the absence of vendor input, can the organisation provide the requisite information and meet its primary and secondary reporting obligations within the identified deadlines?
    - Does the insurance policies of the organisation currently provide sufficient (or any coverage) for business risk?
    - What is the brand communication strategy, should the event become public knowledge? Does this align with the international approach (relevant for multi-national organisations)
    - What is the role of each business unit in responding to the threat, re-stabilising day-to-day business and building resilience and trust with the community and regulator in the aftermath of the event.

"In 2025, Bermuda organisations are operating in markets impacted by continuing geo-political uncertainty, advancements in the adoption of artificial technology (AI) strategies and are subject to increasing disclosure obligations & enforcement activity. Compliance is necessary to improve resilience and ensure operational continuity in the face of the current and future threat landscape."



The final word

Don't get caught up in 2025 focusing on the optics of PIPA readiness. Optics are often illusions and there may be little substance behind many of the published privacy materials introduced into the market over the coming months.

There is a crucial link between business continuity and compliance which is well understood by the most sophisticated organisations. Specifically, compliance with data protection regulations mitigates legal and reputational risks and can further preserve existing revenue and promote revenue growth. In 2025, Bermuda organisations are operating in markets impacted by continuing geo-political uncertainty, advancements in the adoption of artificial technology (AI) strategies and are subject to increasing disclosure obligations & enforcement activity. Compliance is necessary to improve resilience and ensure operational continuity in the face of the current and future threat landscape.

This cannot be achieved via an overly narrow approach to privacy, which is why organisations need to take the time to establish a strategy to embed their privacy programmes into the pre-existing fabric of their business continuity plan and ERM programmes.

BeesMont Law Limited

At **BeesMont Law**, we strive to provide the highest standard of legal service for our clients through our responsive, thorough and innovative approach. We have a friendly and dynamic team who are approachable and sensitive to the commercial and practical needs of our clients, for whom we seek to provide tailored solutions.