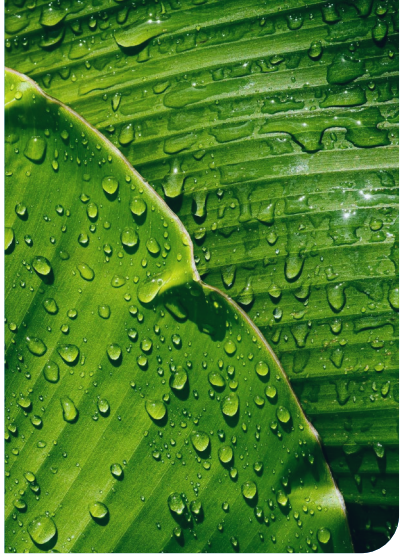
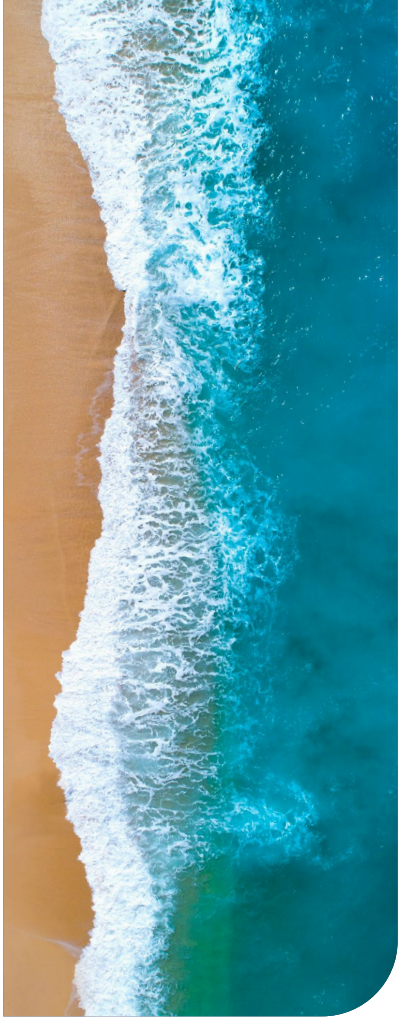
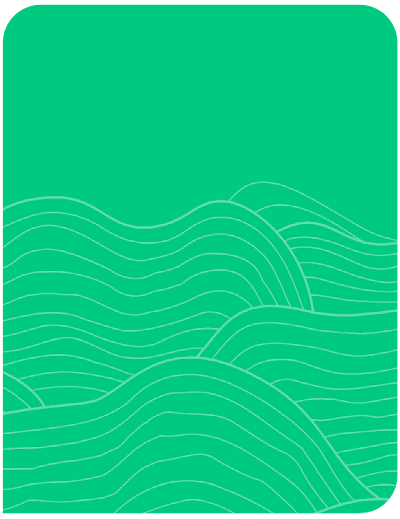






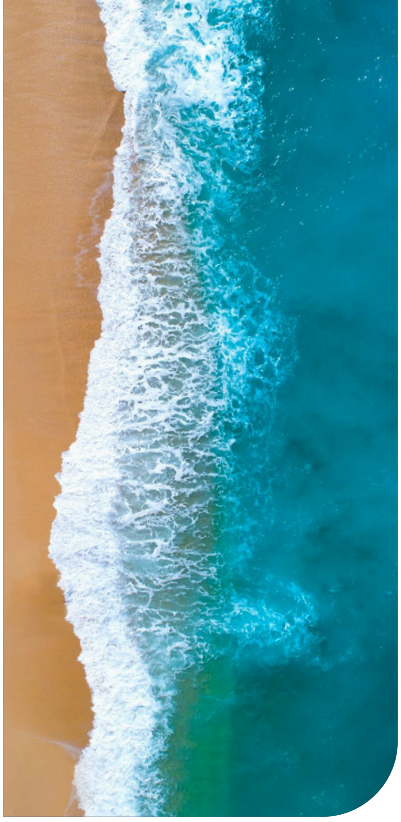
Why PIPA matters:

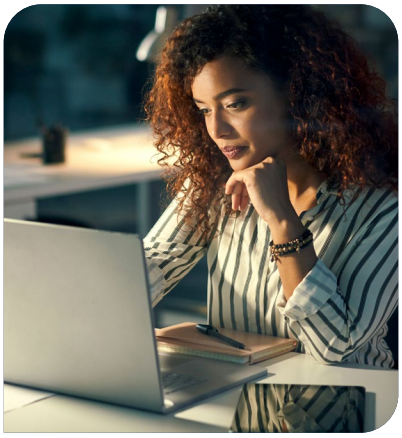
Lessons from global data privacy regulation and enforcement

By Andrew Wychrij, Head of Advisory, Reliance Cyber

RelianceCyber

THOUGHT LEADERSHIP E-BOOK SERIES





Why PIPA matters

INTRODUCTION

We live in an interconnected world, one where the devices we use and the organisations we interact with are hungry for our data. This is far from a new phenomenon and this ever-expanding demand for data from businesses, governments, and other organisations has long since raised serious questions about how personal data should be protected.

That is where regulators have stepped in. Though the genesis of data privacy laws can be traced back decades, the recent era of regulation, spearheaded by the European Union's General Data Protection Regulation (GDPR) that came into force in 2018, has revolutionised the way rules around processing personal data are enforced.

In that vein, Bermuda's Personal Information Protection Act (PIPA) is a new addition to the global data privacy roster but follows in the footsteps of other similar regulations. Modelled after the EU GDPR, PIPA seeks to empower individuals, foster transparency, and hold organisations accountable for data handling. By examining both PIPA – and considering the lessons learned from nearly 6 years of GDPR enforcement – we can extract some interesting lessons from how privacy laws have been applied globally and what this might mean for the future of business operating in Bermuda.

Written by:
Andrew Wychrij, Head of Advisory, Reliance Cyber

PIPA – a new dawn for data privacy in Bermuda

Passed in 2016 and set to come into force on 1 January 2025, PIPA provides a legal framework for the collection, use, and processing of personal information by entities in Bermuda. The act aims to balance the rights of individuals to privacy with the legitimate needs of organisations to use personal data. Under PIPA, individuals gain greater rights to exert control over their information, including the right to access, correct, and delete data collected about them. Additionally, the legislation requires organisations to obtain consent before collecting personal information (with some exceptions) and obligates them to maintain secure data-handling practices.

PIPA is of course a legal requirement, but it's also intended as a tool for building trust in Bermuda's data-driven economy. Industries like insurance, finance, and tourism understandably have a requirement to gather and process personal data – and being able to handle this data responsibly goes a long way to maintaining consumer trust and international partnerships.
Adhering to PIPA's principles means Bermudian businesses will be able demonstrate their commitment to data privacy, which can become a competitive advantage in global markets where compliance requirements are increasingly at the forefront.

PIPA in a nutshell – how to be compliant

The big question for any organisation to which PIPA applies (i.e. all organisations, businesses and the government that use personal information in Bermuda) will be how to achieve and maintain compliance. While there are several requirements that come out of the law, the main points that any organisation should be aware of are as follows:

- **Appoint a Privacy Officer:** Designate an individual responsible for ensuring compliance with PIPA requirements and managing data protection practices. This individual can be responsible for a group of companies or even be an external provider.
- **Consider your legal basis for processing data:** Organisations should ensure that they have a lawful basis for processing data. Often, this will involve obtaining valid consent from individuals before collecting, using, or disclosing their personal information, except in cases where PIPA allows otherwise.
- **Limit data collection and use:** You should endeavour to collect only the necessary personal information for specified, lawful purposes, and use it solely for those purposes.
- **Implement appropriate security safeguards:** Organisations have an obligation to protect personal information with reasonable security measures to prevent unauthorised access, use, or disclosure. This will include basic cyber hygiene methods, like training staff, implementing multi-factor authentication and applying appropriate encryption.
- **Provide access and correction rights:** Allow individuals to access their personal information and request corrections if the information is inaccurate or incomplete.
- **Ensure data breach response procedures are robust:** Organisations must ensure that they can respond effectively to a data breach, including notifying data subjects and regulators as appropriate.

These actions form the backbone of PIPA compliance and, though they may appear straightforward on paper, will require some careful consideration to properly apply.

Lessons from the GDPR: A blueprint for data protection

Looking at the regulation, PIPA draws heavily from GDPR in terms of its measures and ethos in a number of areas. Both regulations focus on:

1. **Empowering individuals:** with rights around access and rectification of their data, as well as restricting or withdrawing consent for processing.

2. **Data breach notification and accountability is a vital requirement:** The GDPR's stringent data breach notification requirements hold companies accountable and prompt them to prioritise data security. Organisations must report data breaches within 72 hours of discovery, pushing them to establish effective security measures. Bermuda's PIPA also mandates breach notification, though stresses that any such notification must occur "without undue delay".

3. **Increased focus on compliance culture:** One of GDPR's most impactful outcomes has been the cultural shift it created within organizations, forcing companies to embed data protection into their operations. PIPA, with its similar focus on consent, purpose limitation, and security, is positioned to have a comparable impact in Bermuda.

4. **Enforcement and Penalties:** GDPR introduced strict fines for non-compliance, with penalties reaching up to €20 million or 4% of an organization's global revenue, whichever is higher. These penalties serve as a strong deterrent and force organisations to take data privacy seriously. PIPA is no different and potentially introduces more stringent penalties in some regard. PIPA provides the possibility of administrative fines and penalty to be issued by regulators, including:

    - A fine not exceeding BM$25,000 or imprisonment not exceeding two years, or both for individuals;

    - A fine not exceeding BM$250,000 for entities.

    - In addition, legal action can be taken against directors, managers, secretaries, other officers, and shareholders of corporate entities in their personal capacity if the offense was committed with their connivance, consent, or because of their negligence.

However, while PIPA emulates GDPR in many areas, Bermuda's Privacy Commissioner will undoubtedly tailor the implementation and enforcement to the island's particular context. There will have to be some consideration given to the fact Bermuda's economy is naturally smaller and less diverse that the EU, and that businesses will need some flexibility and guidance to avoid being overburdened.

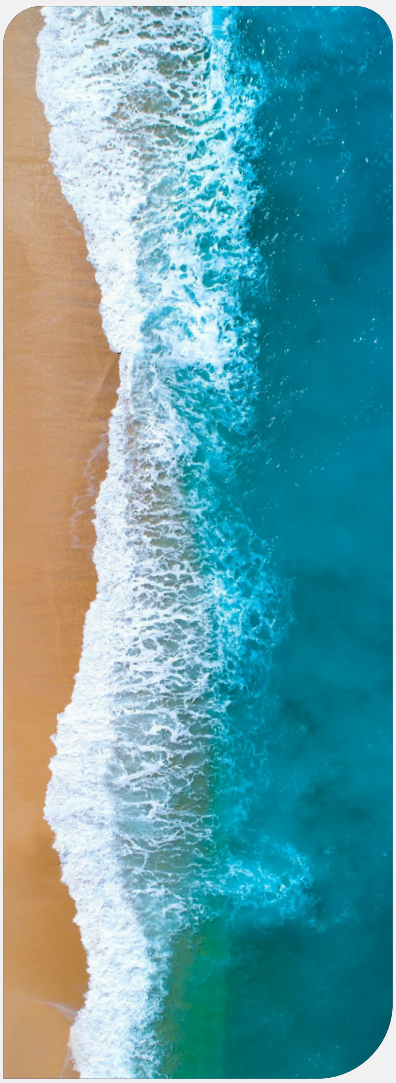
While the work completed over the past six years to clarify aspects of the GDPR will undoubtedly be useful for the Bermuda Privacy Commissioner (for instance, the EU Data Protection Board has regularly issued guidance on specific areas from surveillance to AI) interpretation of the regulation will likely adapt over time.

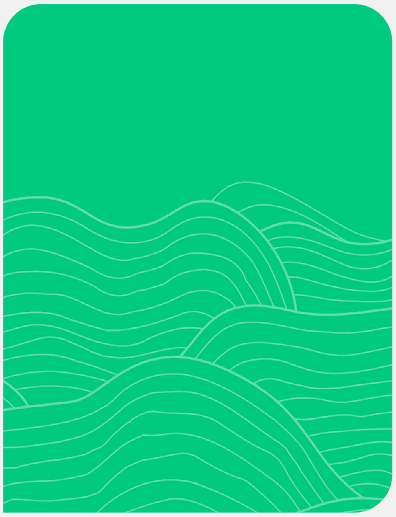
The regulator will need to understand, on a basic level, how strict it wishes to be (and how large the fines will typically be), what it sees as the key areas of concern (i.e. what are the most egregious breaches of the regulation) and how it intends to allocate its resources. On the latter point, it is telling that some EU regulators have focused on bigger, complex investigations, while others have issued a higher volume of fines, but for lower average amounts. Only time – and some case studies – will really help us answer these questions but organisations should pay close attention to the Privacy Commissioner's guidance and clarifications.

A step forward for Bermuda

PIPA marks a crucial step for Bermuda, helping the country join the global movement toward enhanced data privacy. By empowering individuals, fostering organisational accountability, and building a compliance culture, Bermuda's PIPA can protect individuals while simultaneously benefiting businesses through improving trust and accountability.

The GDPR provides valuable lessons in how data privacy can be enforced, individual rights protected, and instilling a compliance culture that Bermuda can emulate. However, PIPA is not simply a GDPR copy and the Bermudian business environment is not an analogue for the EU. As such, there will need to be some careful analysis of trends and cooperation with the Privacy Commissioner's Office to understand how the legislation will grow and develop over time.





Why PIPA matters

Explore the leadership series

RelianceCyber

reliancecyber.com