Walkers

Personal Information Protection Act deep dive

Aug 2, 2024

Key Takeaways

- The Personal Information Protection Act ("PIPA") comes into full force on 1 January 2025. All organisations in Bermuda are expected to be in compliance with it by that date – time is running out!
- The Privacy Commissioner has released the Q3 checklist for PIPA readiness, in this advisory we set out practical tips to help our clients implement the required steps.
- Beware the "global policy". A carefully tailored Bermuda-specific programme is a must.

Background

With less than 6 months to the implementation of the Personal Information Protection Act ("**PIPA**") on 1 January 2025, the Privacy Commissioner has issued the latest "quarterly guide to readiness". This sets out a checklist of deliverables for this quarter's requirements, as summarised below:

As all seasoned privacy professionals know, a checklist will only go so far. Before you can tick off a deliverable, you need the "how". Easier said than done in a jurisdiction with a new law, meaning less people with a genuine history of implementing data privacy laws and a lack of regulatory rulings to lean upon for guidance. With all that in mind, our Regulatory & Risk Team have prepared this customer advisory providing our top practical tips for compliance with each of the three requirements.

Policies and Procedures Compliance Tips

- Do not underestimate policy development time. With 1 January 2025 in mind, factor in time for policy writing, stakeholder sign off and implementation of controls. For larger organisations, factor in significant stakeholder involvement prior to sign-off.
- Where relevant, ensure alignment with your overseas subsidiaries but be cautious of the "global policy" adoption. Local laws will always have quirks, PIPA is no different. The "well its GDPR compliant so it will work here" mindset, is dangerous and inaccurate. For example, many organisations under the EU or UK GDPR regimes seek to rely on the lawful basis of use under Article 6(f), that requires a balance between the legitimate interests of a "data controller" and the interests and rights of the individual. This is not the same as the lawful condition for use under section 6(b) of PIPA. The latter does not factor in the expectations of the organisation, only, in summary, the reasonable expectations of the individual and risk of prejudice to the person. This appears to be a higher hurdle.

- Remember your internal policy is different to your customer facing "privacy notice". Following the privacy notice requirements in Section 9 of PIPA will not assist with your staff facing practical policies and procedures. However, also remember that you collect staff personal information too, so all staff should also receive the privacy notice. It is important to be clear in communications with staff that the policy statement is about your expectations on them; the notice is about their rights in relation to their personal data.
- Use your data mapping and data flows exercises to assign retention periods. Remember, mapping shows what information is where. Data flows refer to how it moves from one place to another:
- By using your mapping and flow exercise outputs, you know where data is, when to review and can establish how and when to destroy it, in accordance with your retention schedule.
- The guiding rule on retention is to destroy when you no longer require the personal information for the purpose for which it was collected. If you are still using personal information for the same or related purposes, you are not required to destroy it "on schedule". Instead, schedule when you will review personal information you have mapped and categorised. To set those review periods:
    - check for minimum retention periods required by law, for example, under AML/ATF requirements; and
    - consider the nature of the personal information in each category. Review periods should be shorter for sensitive personal information, financial information and information that would facilitate identity theft (passport or identity card numbers) than, for example, simple contact information.
- Ensure there are clear lines of responsibility for personal information related tasks. This should include ensuring staff understand, through the handbook, what amounts to valid consent for collection of data, how to ensure personal information collected is logged and categorised, additional controls applicable to sensitive data and responsibility for review of data for retention limitation purposes.
- Consider what supporting documentation you need to implement. A clear and easy to understand general policy statement may be sufficient for the bulk of your staff. Whereas, for those involved in, for example, collecting consent, data destruction, online security etc, a complimenting suite of documents with varying degrees of specificity by relevant topic will best serve the organisation.
- Data destruction has an alternative – anonymisation. If you anonymise personal information, it is no longer "personal" and PIPA obligations fall away.
- If your organisation is closing down, minimum data retention periods will continue to apply. If a liquidator is appointed, the liquidator will have their own data retention periods. Any data not required to be maintained for a minimum legal period, will likely no longer be needed for the purpose it was collected and should be destroyed.
- Communicate the policy statement to staff, consider having them be required to confirm they have read and understood the content. Ensure written policies and procedures are on your intranet or available in physical form in the office.

Training Compliance Tips

- If you can, ensure the training session is in person. Desktop training carries the risk of staff getting distracted and not paying attention. Make the training mandatory, with follow up for staff who cannot, or do not, attend.

- For those staff that use personal information directly, conduct scenario-based training. This should include practical steps and testing how they would implement the policies and procedures adopted, through mock documents and roleplay.
- Consider following the scenario-based training with a written test to ensure the learning has been understood.
- Consider a third-party provider who can conduct workshops with your staff using real or theoretical use cases for data, data flows and sharing. These can be immensely helpful for practical implementation.
- Following training sessions, select a cohort of people across the organisation of different levels and in different business units to provide feedback. Factor the feedback in to future training sessions. Often, more genuine feedback can be obtained from a conversation than trying to solicit written feedback from busy people – schedule some time in diaries.

Outsourcing and Service Providers Compliance Tips

- Remember your organisation remains responsible for compliance with PIPA at all times, you cannot outsource that responsibility.
- Conduct due diligence on vendors before agreeing to transfer data to them. This should consist of a questionnaire or similar to allow for consistency of assessment, it should look at the vendors policies and procedures for data privacy, data sharing and cybersecurity.
- Ensure your privacy notice to customers adequately describes who customer information is shared with and where, and that includes any onward sharing by the service provider. For example, with regulators and law enforcement in that jurisdiction.
- Obtain and review all contracts with outsource and service providers. Legal counsel can check the contract:
    - adequately specifies the policies, procedures and controls the third party is required to maintain to ensure the ongoing security and confidentiality of personal information provided;
    - sets out the purpose of the information sharing, including aims of, and necessity for, sharing;
    - requires compliance with all applicable privacy laws;
    - requires the maintenance of appropriate risk management standards and controls;
    - requires the third party to provide notice to you of any onward sharing arrangement or obligation;
    - requires the third party to provide updates and notification regarding ongoing maintenance of technological and operational capacity to adequately protect personal information;
    - requires disclose of any adverse events such as cyber attacks or data leaks;
    - contains data information and security KPIs; and
    - requires the maintenance of adequate business continuity plans and disaster recovery plans.
- Monitor the relationship to ensure agreed standards are being met and have a process in place to alert the relevant person (privacy officer or compliance) that a contract is due for renewal such that it can be assessed from a privacy perspective.
- For overseas transfers, section 15 of PIPA applies. Organisations must conduct an assessment of the protection provided by the third party in relation to personal information. This will include considering the equivalence of the law in place in the jurisdiction to PIPA. However, we recommend wider considerations than black letter law. Some jurisdictions have higher incidents relating to large

scale data breaches, worse cybersecurity reputations and less protection of personal information as against state bodies, despite laws that look robust on paper.

- For overseas transfers, check whether the Privacy Commissioner has recognised certification mechanisms in place. For example, the Asia Pacific Economic Corporation Cross Border Privacy Rules System is recognised for overseas transfers.
- If the jurisdiction cannot be assessed as offering comparable protection, PIPA remains flexible and allows for an organisation to mitigate risk through contractual mechanisms and corporate codes of conduct.

Conclusion

Walkers Bermuda can assist with all aspects of compliance with PIPA, including training, policy and procedure development, privacy notice drafting, delivering in depth workshops and advising on terms and conditions and data sharing with external service providers, intragroup entities and practice groups and overseas transfers.