



Bermuda privacy survey results

Rights and obligations

June 2021

Content

Introduction	03
Introducing privacy regulations in Bermuda	04
Implementing a privacy program	06
Risk based approach to privacy	07
Training and hiring privacy employees	08
Appointing a privacy officer	09
Overseas third party transfers	10



Introduction

Technological developments, changing products and services and globalisation have resulted in organisations collecting more consumer data than ever before and expanding data security risks commensurately. The COVID-19 pandemic accelerated these changes and the dependency on technology through the shift to remote working, online sales and inquiries, and the increased need for the sharing of personal health information. Consumers have become savvier and with Global Regulations, such as the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and local regulations, such as the Personal Information Protection Act (PIPA), have more rights over the personal information companies hold about them.

Globally, organisations have recognised the changing landscape and the new challenges brought on by it. A Cisco survey found that 93% of organisations found their privacy teams helped them navigate the challenges brought on by COVID-19. Further, the study found that the average privacy budget had doubled in the past year while retaining a high business value. When asked about privacy legislation, almost 80% of these companies indicated that the privacy legislations had a positive impact.

But the work isn't done. A KPMG global CIO survey of all sectors and specifically the insurance sector, found that 45% of companies in the insurance industry are planning to accelerate transformation to re-emerge from COVID-19 and, for all sectors, the most important technology investment in light of the new reality relates to insurance and privacy.

KPMG in Bermuda (KPMG) has conducted a survey to identify how our local Bermuda market is preparing for changes in privacy. This will help identify common pain points and solutions in the transition to compliance with changing regulations in a changing world. KPMG believes that trust is vital to any initiative involving personal data. Many businesses are recognising these challenges as we move toward a new normal and hope to build a strong community of trust locally in Bermuda and as part of a wider global network.

Introducing privacy regulations in Bermuda

Organisations are looking to understand exactly how privacy regulations are going to impact their business. KPMG has conducted an island wide survey to research the common struggles and attitudes towards privacy regulation in Bermuda.

Our respondents range from wide reaching international organisations to small local businesses, covering all industries from insurance to financial institutions to hospitality.

By far, the most encouraging data point discovered during our survey was that 100% of our respondents believe that privacy regulation is good for our island community. However, 25% of our respondents said that they did not believe privacy regulation will be beneficial specifically to their organisation. This shows a divergence between our community and corporate perspectives.



100%

of respondents believe privacy regulation is good for Bermuda as a community



of respondents had little to no understanding or were neutral on their understanding of the privacy regulations.

Privacy regulation is new to Bermuda and with the passing of the Personal Information Protection Act (PIPA), many organisations in Bermuda are dealing with the realities and difficulties of privacy for the first time. It is not surprising that 75% of our survey respondents said, they had little to no understanding or were neutral on their understanding of privacy regulations, and how these changes in legislation would impact their businesses going forward.

Some of these responses may be due to the fact that guidance has yet to be issued on all aspects of PIPA. Businesses will hope that the detailed guidance will assist implementation, and remediation where necessary. A robust and effective privacy program will not only increase trust for your organisation within our island community, it will also lift Bermuda up as a trustworthy and safe place for personal information to the whole world.



How best to approach compliance with a new regulation can be unsettling. Tackling the challenge of building a privacy program will look different for each organisation. The flexibility of PIPA is one of its most positive aspects. Building a strong privacy program, using the privacy principles outlined in PIPA, will allow your program to work with your business, while remaining agile to support the changing global privacy requirements and needs of your data subjects.



of respondents do not have a
PIPA readiness plan



of respondents do not think
larger fines will change their
approach to privacy

Global privacy legislation has seen a greater tendency to comply when higher fines are imposed. Larger fines and penalties have also been shown to have a greater impact on organisations to implement strong privacy programs. This is most likely due to the fact that larger penalties have gotten more board members actively involved in the process of building a privacy program. This aids in driving a higher budget for privacy related maintenance and projects. However, 45% of respondents do not think that larger fines will change their approach to privacy and another 40% remained neutral on if fines would change their approach.

80% of respondents feel supported by the Board of Directors and upper management within their organisation when it comes to implementing privacy initiatives. With a positive tone at the top, Bermudian organisations may successfully implement programs without an additional threat of large penalties.

Implementing a privacy program

Spending on a privacy program can range greatly from organisation to organisation. There is no one-size-fits-all approach to privacy and that can be a good thing. Each organisation has the ability to assess their exposure and privacy risk and apply appropriate safeguards to minimise their risk.

Uncertainty around your organisation's expected spend may be due to the fact that additional guidance has yet to be issued for your organisation's particular circumstances. However, protecting personal information is not always about having the latest and greatest or most expensive technologies.

Protecting personal information is not always about having the latest and greatest or most expensive technologies. It is about implementing the appropriate procedures for your business model that will best protect your data subject's information.

35% of our respondents are unsure of how much they will need to spend on a privacy program. Your privacy spend will depend on the type of personal data your organisation processes and the business practices your organisation already has in place. The safeguards you choose to implement can range from encryption software to a simple lock on a filing cabinet or office door.

25% of respondents expect to spend zero dollars on a privacy program. While spending zero dollars to maintain a privacy program is possible, your organisation is probably allocating privacy costs to another area of your organisation. For example, your firm might have a robust business continuity and disaster recovery program, or your business has documented information security policies and procedures that also cover personal information.

Your organisation may be receiving personal data that is not relevant for business operations – data minimisation tactics can be implemented to reduce your firm's privacy risk.



of respondents are unsure how much they will need to spend on a privacy program



of respondents expect to spend zero dollars on a privacy program

Risk-based approach to privacy

Businesses should take a risk-based approach when considering how to implement their privacy programs. Privacy programs allow for great flexibility and for safeguards to be applied proportionally to an organisations' specific contextual risks. 90% of our respondents have developed a risk-based approach towards privacy.

When considering how to proportionally and appropriately address privacy risk, businesses should also consider their overall risk appetite. They should ask themselves, how privacy risks impact the organisation's

overall risk profile and how any existing safeguards are helping to mitigate that risk. 85% of our respondents have defined their privacy specific risk appetite. Organisations should ensure their privacy risk appetite aligns with their overall business objectives and risk profile.

Identifying your specific privacy risks is a key step in implementing proportional controls. A risk based-approach, applied consistently, balances your business goal and cost of controls to create your ideal privacy environment.



90%

of respondents have developed a risk-based approach towards privacy



85%

of respondents have defined a risk appetite for privacy risks



15%

of respondents plan to make privacy related hires



35%

of respondents are open to hiring new personnel to assist with privacy



50%

of respondents do NOT plan to make any privacy related hires

Training and hiring privacy employees

Organisations will need to have a locally accessible privacy contact to interact with the Privacy Commissioner, build out a proportional and sustainable privacy program, and handle local data subject requests. Depending on your organisation's size and the amount of personal data you process, there can be very differing approaches to finding the appropriate privacy personnel.

50% of our respondents do not want to make any new hires that are solely privacy related. This makes sense for a smaller business that processes small amounts of personal data, or for businesses that believe they already have talented privacy professionals in house. 15% of respondents do plan to make privacy related hires. Privacy professionals can have a variety of roles within the organisation and can help enhance your business objectives.

Even if your organisation does not plan to make any hires, training your existing personnel should be a top priority. Having annual privacy and data protection training is one of the best ways to protect personal information in your business. Ensuring that your employees understand the importance of their role is paramount to protecting personal information.

Employers should consider the ongoing privacy considerations for their business. Once you have a privacy program, management should know who will be in charge of running that program and making appropriate updates as necessary.

When considering the appropriate candidates, employers should consider how and why they are collecting personal information. An organisation may need additional legal expertise to assist with contracting and data transfers. Businesses might carry both personal information and sensitive business information that requires support from both a cyber security and privacy perspective. Your business processes that require personal information may be very specific to your organisation and you will need someone with extensive industry knowledge. Building your privacy team to enhance your business objectives will ensure that privacy is an integral and respected aspect of your organisation.



Appointing a Privacy Officer

A Privacy Officer can have many functions and can sit in which ever part of your organisation makes the most sense for your business structure. For example, if your organisation holds personal data that is mainly employee data, it might make the most sense for someone on your HR team or sitting in the HR department to fill the role of a Privacy Officer.

Finding the right person for the role can be challenging, the best place to start is to identify the personal information your organisation uses and the business purposes it is being used for. A Privacy Officer should understand the businesses' processes that require personal data and how that data moves across the organisation and potentially to third parties.

It is important that the Privacy Officer is of a high enough rank in the organisation to properly implement and oversee a privacy program. The Privacy Officer will need support from the Board of Directors and upper management. Setting the tone at the top is vital to building a successful privacy program.

Consider your employees, has anyone in your business expressed an interest in privacy? Is there someone with capacity to take on this role or should you consider a new hire or outsourced model?



of respondents ranked appointing a Privacy Officer as the most difficult hurdle to becoming compliant with PIPA

Overseas third party transfers



Comparable country

Must be recognised by the Minister and, at a minimum, meet all standards required in PIPA



Certification mechanism

Commissioners general powers to introduce certification mechanisms and recognise certifications of third parties.



Binding corporate rules (BCR)

A set of data protection policies, processes and standards, together with contractual provisions that bind the entities and employees of an international organisation to adhere to them.



Contractual mechanisms

Contractual clauses that bind a non-Bermudian entity to provide a comparable level of protection.



Assessed and reasonably considered to be:

- small scale;
- occasional;
- unlikely to prejudice the rights of an individual.

PIPA is very prescriptive on its rules governing overseas data transfers. Organisations can use one or more of the five approved routes to perform overseas transfers. 53% of respondents still perceive a moderate to high level of difficulty in performing safe overseas personal data transfers.

The process of identifying a comparable country requires the Minister to recognise a jurisdiction as "comparable" on recommendation from the Office of the Privacy Commissioner. A comparable country will have to meet all standards required in PIPA and any other criteria the Minister and Commissioner deem appropriate.

An appropriate certification mechanism has been identified for businesses to use, easing the ability for Bermudian organisations to safely transfer data to overseas third parties. The Office of the Privacy Commissioner for Bermuda has recognised the Asia Pacific

Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System as a certification mechanism for transfers of personal information to an overseas third party.

Binding corporate rules and contractual mechanisms can be applied in contracts with third parties. Organisations should contractually obligate their third parties to be compliant with PIPA's regulations when processing personal data. They can also include oversight requirements and reporting requirements to businesses that can have assurance that their third parties are handling personal data properly and they remain compliant with PIPA.

Finally, an overseas data transfer can also be performed if it is assessed and reasonably considered to be small scale, occasional, and unlikely to prejudice the rights of an individual.



53%

of respondents perceive a moderate to high effort to safely perform overseas transfers of personal data

How we can help

At KPMG in Bermuda, we are helping organisations to address their privacy challenges, our professionals adopt a structured and flexible approach to meet the needs of your business. The areas where we add value, include:

- **Assessments** - Provide an independent assessment of current risk profile and how this compares to desired state.
- **Design** - Design a privacy compliance program to meet requirements of legislation.
- **Strategy** - Develop a pragmatic privacy strategy and gain buy-in from senior management.

- **Monitoring** - Support you in maintaining your privacy control environment.
- **Operations** - Provide ongoing support and advice to assist you in operating your control environment.
- **Implementation** - Support the implementation of robust and sustainable processes, policies and controls to allow you to mitigate your privacy risk.

For more information on KPMG's Privacy services and how we can help, please contact us today

Ian Gardner

Director, Advisory
+1 441 294 2721
iangardner@kpmg.bm

**Katy Gloth**

Assistant Manager, Advisory
+1 441 294 0771
katherinegloth@kpmg.bm



kpmg.bm

© 2021 KPMG, a group of Bermuda limited liability companies which are member firms of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The information contained herein is of general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.