Perspectives on Bermuda's Personal Information Protection Act – Why Does it Matter?

Ensure compliance with PIPA

Bermuda created our own Personal Information Protection Act (PIPA) of 2016 to establish local legislation and regulations, essentially to meet EU data privacy standards. PIPA received Royal Assent on July 27, 2016 and is expected to go into force once an independent Privacy Commissioner is appointed to ensure the aims of PIPA are being met and oversee compliance.

Once the Privacy Commissioner is appointed it is expected that there will be a period of consultation with industry in advance of final implementation or any enforcement action.

Operating in Bermuda, an international financial centre, forces business people to remain abreast of the constantly changing landscape of global regulations. These regulations, almost invariably, are condensed into acronyms, drowning us in a sea of alphabet soup: AML…KYC…ATF…FATCA….BEPS…CFATF…CRS…and the list goes on. Of course, who could ever forget the most dreaded acronym in recent memory that consumed extensive resources and time: Y2K?

Two new acronyms entered our regulatory lexicon in the past two years: GDPR and PIPA. These regulations both address the need to protect the privacy of individuals in the age of the internet and the constant flow of digital information.

The General Data Protection Regulation (GDPR) was adopted by the European Union (EU) and came into force on May 25, 2018. The GDPR protects EU citizens by giving individuals more control over how companies use their personal data, usually referred to as "PII" or Personally Identifiable Information.

How many readers started receiving interesting emails from online companies disclosing their privacy policies in April and May 2018? How many have been suddenly forced to review and acknowledge privacy policies in pop-up windows before being able to proceed with normal browsing? These actions by companies were directly related to GDPR and the potential risk of significant fines for noncompliance: the greater of 20,000,000 Euros or 4 percent of worldwide revenue.

A look at Bermuda's PIPA

Bermuda created our own Personal Information Protection Act (PIPA) of 2016 to establish local legislation and regulations, essentially to meet EU data privacy standards. PIPA received Royal Assent on July 27, 2016 and is expected to go into force once an independent Privacy Commissioner is appointed to ensure the aims of PIPA are being met and oversee compliance. Once the Privacy Commissioner is appointed it is expected that there will be a period of consultation with industry in advance of final implementation or any enforcement action.

Why are these regulations so important? Globally recognized companies have been hacked leaving millions of records of PII compromised including Equifax (146 million records) Under Armour (150 million) and Yahoo! (three billion records). While these numbers may seem high on initial glance, we need only reflect on our daily activity and how we communicate with each other. We are constantly on devices connected to the internet, generating and sharing information, leaving a digital footprint. This graphic shows the staggering amount of data that is generated each minute on the internet.

In this day and age, every organization needs to understand the information that drives the components of its business model; the organization's information lifecycle.

This lifecycle starts with the creation and/or acquisition of information. Organisations must understand what data is being collected and created, who it is from, how it is obtained, and through what channels? Next, the organization needs to understand where data is stored – both within and outside the company, and in which systems, including paper-based filing systems?

The organization then needs to develop a complete picture of how the data is being used, what it is being used for, and who is using it? Data is frequently in motion or transmission, being shared – inside and outside the company, sometimes across multiple jurisdictions. Last, but certainly not least, the organization needs to decide on options for archiving and ultimately disposing of data. How is data retained – both by the company and by third parties, for how long, and how is it destroyed?

Policies, procedures, and controls provide the framework for effectively implementing the elements of an organization's information lifecycle. Policies are created to meet the organization's legal and regulatory obligations. Procedures describe step-by-step processes that enable the firm to carry out workflows in a manner that is consistent with the policies. Controls are designed and tested to provide evidence and comfort to management and the board of directors that the policies are, in fact, being followed in a consistent manner.

Limit, protect and respect!

There are three principles to apply when dealing with personal data: limit, protect and respect.

Limit the personal data you collect to include only what you need to perform services. Be diligent and judicious about what you collect and make sure you only use that information for the designated business purpose.

Protect the data that you collect through effective procedures and controls. Access should be restricted to only those who need the information. Flexible and remote working on laptops, tablets, phones, and reading printed materials on airplanes or in transit create potential exposure of sensitive information.

Respect the rights of the individuals whose personal data you collect, store and share. GDPR requires transparency, the ability for individuals to opt in or not, and providing individuals the right to be forgotten.

Board governance

Ultimately, the board of directors and executive management of each organization must understand and embrace the dynamics of privacy in the age of GDPR and PIPA. Data privacy is a critical element of risk that must be incorporated in the Enterprise Risk Management framework for every organization.

Oversight of information technology and digital assets is a growing focus for boards and with the pressures of GDPR expectations for director performance are increasing. According to PwC's 2018 Annual Corporate Directors Survey, more than four out of five directors (83 percent) say their board is very or moderately involved in monitoring the status of major IT projects. Close to 75 percent say the same about the company's digital strategy.

With the major security breaches involving data privacy, and new governmental regulations — many more directors also say they are engaged with overseeing or understanding big data. The percentage of directors saying their boards are at least moderately involved jumped to 65 percent from 51 percent in 2016. Directors also report being much more involved in overseeing how their company leverages and monitors social media. Both of these areas have shown substantial increases since 2016.

The principles for handling personal data in a prudent manner provide guidance to organizations. The board and executive team must give clear direction and set the tone regarding the importance of data privacy and establish an appropriate operational framework, including appointing a data privacy officer (DPO). Effective policies and procedures, tested on a consistent basis through well-designed controls, can ensure that the organization is meeting global standards.

For a deeper conversation connect with Chris.Mills@pwc.com, Director, PwC Bermuda