Article

Understanding PIPA: Why Do We Need Privacy Legislation?

Authors: Julie McLean, Director | **Andrew Barnes,** Associate | **Sarah Blair,** Associate

In a four-part series, Conyers will be diving into different topics relating to Bermuda's privacy legislation, including: how do we prepare for PIPA, the role and requirements of privacy officers and what are our rights as individuals? In this first article, Conyers provides an introduction to PIPA, why we need it and what is its purpose.

In recent years, privacy and data protection are hot topics. It's not difficult to see why: as technology has evolved, so has the way that organisations store, use and process our data and personal information. Sometimes a company's use of personal data is straightforward and transparent: a company takes and stores a customer's information for the purpose of processing their sales order. But what of the times when their use is more opaque? Or when the data collected is far broader than what you expect or is not proportionate to what the company actually needs? What of data breaches, when our details are accessed by a hacker? Or where it's inaccurate?

Beyond the practical issues, there's also the moral and philosophical: is the use of our data helpful or harmful? Take the use of data to improve targeted advertising as an example. Perhaps it speeds up our shopping experience and helps us find exactly what we're looking for (helpful) or does it instead manipulate our choices, our autonomy, and serve the company's wants rather than our own (harmful)?

It's in this context that countries around the world have developed and implemented data and privacy legislation. Bermuda is no exception: in 2016 it passed the Personal Information Protection Act (commonly referred to as "PIPA") although its substantive provisions are yet to come into force.

Generally, privacy legislation (PIPA included, when it comes into force) seeks to, on the one hand, respect an organisation's legitimate purposes for the data, while setting parameters for how companies should store, use and protect it, and, on the other hand, empower individuals to know how their data is being processed and used, by whom and why, and to take certain actions in respect of it.

To properly protect data, you need both 'data privacy' and 'data security'. Even though these two terms look similar, they are different. 'Data privacy' focuses on the rights of individuals in respect of their personal data, including the purpose of data collection and processing, and the way organisations handle, store and use the personal data. 'Data security' relates to protecting the data: implementing safeguards in order to prevent any third party from unauthorised access to the data, or any intentional or unintentional alteration, deletion or disclosure thereof. This includes preventing malicious attacks and the exploitation of stolen data (data breaches or cyber-attacks such as the theft of data that led to the Paradise Papers). PIPA is primarily designed to ensure data privacy although it does place an obligation on organisations to ensure the data they collect is kept secure.

As noted, one of the primary purposes of PIPA is to protect the privacy of individuals with respect to their personal information in the custody or control of institutions. PIPA does not define privacy explicitly but rather defines "personal information" and sets out privacy rules for institutions to follow for the collection, use, disclosure, maintenance, retention, security and disposal of personal information. "Personal information" is broadly defined and means "any information about an identified or identifiable individual" (i.e. a natural person, whether they are explicitly identified e.g. by name or where their identity is identifiable from e.g. a piece of information, such as their social insurance number). PIPA also deals with 'sensitive personal information', meaning "any personal information relating to an individual's place of origin, race, colour, national or ethnic origin, sex, sexual orientation, sexual life, marital status, physical or mental

disability, physical or mental health, family status, religious beliefs, political opinions, trade union membership, biometric information or genetic information". Sensitive personal information is, understandably, subject to greater obligations and restrictions.

To understand how PIPA is to be used, it's helpful to think about its general underlying principles. These are that personal information shall be:

(i) used fairly and lawfully;
(ii) used for limited specified purposes;
(iii) adequate, relevant and not excessive in relation to the purpose or purposes for which it is used;
(iv) accurate and, where necessary, kept up to date;
(v) not be kept for longer than is necessary for its use;
(vi) used in accordance with the rights of individuals;
(vii) kept securely; and
(viii) only transferred to third parties (including international transfers) where there is a comparable level of protection.

These principles are aimed at ensuring transparency, accuracy, proportionality and security in respect of an organisation's use of personal information in Bermuda, while providing a level of personal autonomy and control to individuals in respect thereof.

Now we understand the context and purpose of PIPA, the next part in this Conyers PIPA series will consider what organisations PIPA applies to and what organisations can do to prepare for PIPA.

Disclaimer: Nothing in this article constitutes legal advice and is for general purposes only. If you would like to obtain legal advice on PIPA, please contact the Conyers team:

Authors:

Julie McLean
Director
julie.mclean@conyers.com
+1 441 299 4925

Andrew Barnes
Associate
andrew.barnes@conyers.com
+ 1 441 278 8054

Sarah Blair
Associate
sarah.blair@conyers.com
+ 1 441 279 5335