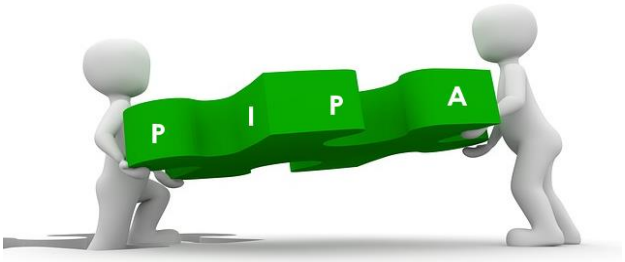
The Personal Information Protection Act-2016 (PIPA)

What organisations should know about protecting personal information under the PIPA

What is the PIPA?



Solving the Privacy Puzzle

The PIPA provides individuals with important rights over their personal information and creates duties for all organisations that use any personal information.

The PIPA is scheduled to come into force in 2018 and organisations should begin privacy compliance preparations now, so to avoid potential breaches of the legislation.

Protecting Personal information has Business Benefits

Pro-active personal information handling practices are good for business. They create trust between an organisation and its employees or clients. The prevalence of data breaches and the wider issue of cybersecurity as a whole, are making people more concerned about the way organisations treat their personal information. Information security is in fact a key component of the PIPA.

What does the PIPA require?

The PIPA is based on internationally accepted Privacy Principles that have formed the basis of privacy legislation in many jurisdictions, including Bermuda's competitors.

In practical terms this means:

1. **Organisations must have a legitimate or lawful need for using personal information**. This includes the consent of the individual, or for the performance of a contract.
2. **Organisations must be accountable and transparent.** They must inform individuals what personal information they use, why, and if it is being shared. This is usually done through a privacy notice. Individuals must also be provided with access to their personal information and organisations must identify someone to act as the Privacy Officer, as the point of contact for the public and for the Privacy Commissioner.
3. **Minimal and Limited Use of personal information.** Organisations should only collect the minimum amount of personal information necessary to provide services and must use the personal information only for the stated purpose.
4. **Security.** Organisations must keep the personal information they have secure. This is particularly important where sensitive personal information is concerned, as additional safeguards may be needed. There are also requirements to report material data breaches, both to the Privacy Commissioner and to the individuals concerned.

5. **Organisations must ensure the data is accurate, up to date and retained no longer than is necessary.** This is a good practice as organisations are responsible for the personal data held in case of a breach.
6. **Organisations are responsible for the personal information that they transfer onwards**. This applies to transfers to any third parties whether they are local or outside of Bermuda. There are additional obligations when transferring personal information outside Bermuda.
7. **Penalties may apply.** Where there are violations of the Act, Directors and Officers of organisations can be held personally liable.

What can you do to get ready? Think PIPAPREP

Prepare a privacy program demonstrating the organisation's commitment to address PIPA compliance.

Identify the personal information that your organisation holds, uses and transfers, and define the privacy risks and obligations accordingly.

Provide the appropriate policies, procedures, notices, contracts and forms as required, and appoint a **Privacy Officer** for the organization. Develop appropriate processes for individuals to access their personal information and exercise other rights.

Address training needs and create staff awareness about PIPA related policies and procedures.

Protect the personal information you hold, whether it is in physical or electronic files. Consider security practices at physical locations and for computer based systems and create an incident response plan.

Respond promptly to any incidents where personal information has been compromised by executing the response plan, including any obligation to report to the Privacy Commissioner.

Evaluate and monitor your privacy preparedness on an ongoing basis and keep evidence of all steps being taken.

Promote your privacy practices to your clients through a privacy vision statement. Studies have shown that clients prefer dealing with organisations that are serious about protecting their personal information.

General Data Protection Regulation (GDPR)

Some businesses in Bermuda will be affected by the introduction of the EU GDPR on May 25, 2018.

Those Bermuda organisations that *target goods or services to individuals in the EU*, *monitor the behaviour of individuals inside the EU, or have offices in the EU* must consider their position.

Fines are onerous and the new regime has a sufficient number of material changes to warrant a review of all privacy policies and procedures.

Gateway has an experienced and knowledgeable team supported by some of the world's leading Privacy Specialists who can help solve your PIPA and GDPR challenges.

Gateway also offers cybersecurity and software solutions to streamline privacy implementation.

For more information, please call (441) 292-0341 or e-Mail: info@gateway.bm

---