PIPA for Business Owners

Cybersecurity Governance Board:

Alexander White, Privacy Commissioner, Office of the Privacy Commissioner

Dr. Marisa Stones, Sr Information and Privacy Analyst, Government of Bermuda

Agenda

- Personal Information Protection Act 2016
- What is a Privacy Programme?
- Q&A

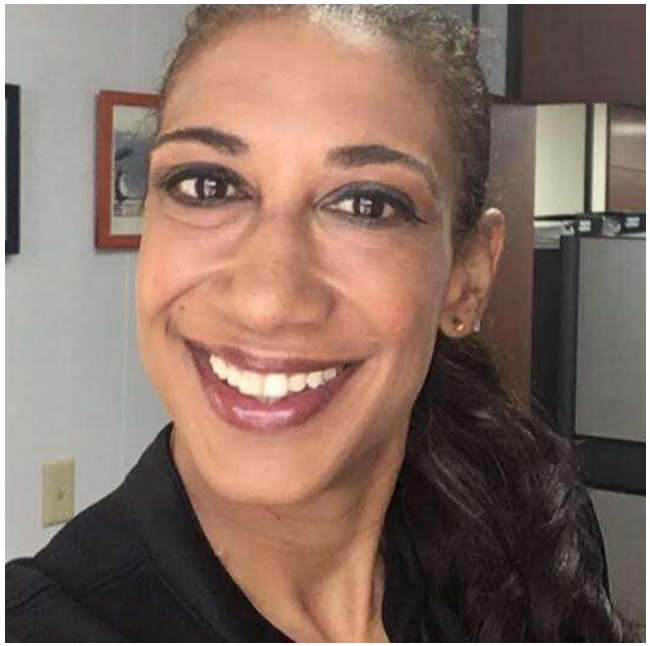
Presenters

Alexander White,

Privacy Commissioner, Office of the Privacy Commissioner

Dr. Marisa Stones,

Sr Information and Privacy Analyst, Government of Bermuda



Personal Information Protection Act 2016 “PIPA”

What is Privacy?

There's the policy wonk's definition…

- "The right to be left alone"
- "No one shall be subject to arbitrary interference"
- "Respect for private and family life"
- "Protection against intrusion"
- "Respect for the autonomy of individuals

What is Privacy?

And there's what it really means:

- Privacy is…
  - the management of information that relates to an individual
- For that individual, privacy is about controlling the information about themselves
  - In modern times, more and more people are participating in an individual's privacy

How do you ensure an individual is in control of their privacy?

Provide Information	Give them information so they can make an informed choice
Choice	Give them a way to tell you what their choice is
Keep Promises	Make sure you abide by the promises that you make

PIPA – Personal Information Protection Act

“Minimum Requirements”

- Responsibility and compliance
- Fairness
- Proportionality
- Integrity
- Security

Additional Requirements

- Purpose limitation
- Conditions for using personal information
- Privacy notices
- Sensitive personal information
- Personal information about children

Individual Rights

- Access
- Rectification
- Blocking
- Erasure or Destruction

What is a Privacy Programme?

Privacy Programme Checklist

Privacy Officer	The Privacy Officer is responsible for developing the organisation's privacy programme and for communicating with the Office of the Privacy Commissioner and the public
Inventory	Conducting an inventory and classifying (or, "mapping") what personal information is used
Policies & Procedures	Documenting personal information use practices in policies and procedures
Training & Awareness	Providing appropriate training and awareness to staff or others who access data
Privacy Risk	Analysing the privacy risk in context, utilizing tools such as "Privacy Impact Assessments," and identifying protective measures
Incidents	Developing an action plan to respond to incidents or potential breach of security
Rights Request	Developing procedures to respond to PIPA Rights Requests

Privacy Officer

The Privacy Officer is responsible for ensuring that the organisation develops appropriate measures and policies to give effect to its obligations and to the rights of individuals under PIPA.

Privacy Officer's contact information listed in privacy notices, so the privacy officer must be available to respond to questions from individuals and/or requests to exercise PIPA rights.

They are "responsible" for compliance, but may delegate the actual duties that make up ensuring organisational compliance.

Inventory

Know what types and quantities of personal information you hold

Include details

- type of data ("health," "financial," "educational," etc.)
- more specific sub-categories
- individual data elements ("health insurance number," "credit score," "grade point average," etc.)

Track the flow of information within the organization

- For example: a paper intake form received by the receptionist → scans the paper to create an electronic copy → stores the paper version in a particular filing cabinet → electronic version saved in a particular computer hard drive or cloud storage drive

Policies and Procedures

Document how you intend to use personal information

Include policies that outline:

- high-level business purposes to be accomplished
- conditions of use under PIPA section 6
- type of data to be collected and used
- appropriate standards of protection

Privacy Notice

- personal information is being used
- purposes for which personal information is or might be used
- identity and types of individuals or organisations to whom personal information might be disclosed
- identity and location of the organisation, including information on how to contact it about its handling of personal information
- name of the privacy officer
- choices and means the organisation provides to an individual for limiting the use of, and for accessing, rectifying, blocking, erasing and destroying, personal information.

Employee documentation:

- procedural instructions for employees, staff, or anyone who may access personal information

Training & Awareness

General awareness training

- on a recurring, often annual, basis
- covers basics on understanding personal information risks
- help organisations identify privacy risks, since employees may spot problems in the course of their work

Role-specific training

- relates to the particular issues of an employee's specific tasks
- for example:
  - different training for human resources personnel than for sales personnel
  - different for cashiers than general managers

Vary in frequency or intensity according to the type of personal information used and the risks

Privacy Risks

Context	analyse privacy risk in their specific context
PIA	walk through a business process to identify risks or gaps identify what protective controls would be needed identify when they share information with other organisations what contractual mechanisms or other protections are needed
Controls	will vary based on the type of personal information and what actions would be reasonable give special consideration to the risks involved with sensitive personal information

Incidents

Incidents could include mistakes when sharing personal information or a breach of security

Develop action plans in advance for how you will respond

- Who to notify within the organisation
- Identify who will make decisions regarding incident response
- Identify vendors that assist with breaches of security (*before* a breach actually occurs)

Security Breach

- Privacy officer would be required to notify the Office of the Privacy Commissioner and any individual affected
- Develop template communications or lists of contact information

Rights Request

PIPA Part 3

- right to contact organisations to request access to their personal information
- request correction or destruction of their data
- block its use, in certain circumstances.

Response to Requests

- organisations must be ready to respond to these requests
- employees such as receptionists, cashiers, or call centre operators who receive requests should know where to direct them
- section 20 of PIPA contains detail on specific actions, such as acknowledging requests in writing and meeting the time period for responding to requests

Documentation:

- document your due diligence and factors entering into their reasonable judgements to show good accountability

Q&A

For More Information

Alexander White

Office of the Privacy Commissioner
PrivCom@privacy.bm
www.privacy.bm

Dr Marisa Stones

Government of Bermuda
mastones@gov.bm