Fact Sheet: Privacy Management Program

The *Protection of Privacy Act* (POPA) requires public bodies to establish and implement a privacy management program (PMP).

Purpose of a PMP

Section 25 of POPA requires that each public body establish and maintain a PMP, which consists of documented policies and procedures that promote the public body's compliance with its duties under this Act.

A PMP is an evolving set of policies, procedures and tools developed by a public body to ensure privacy is protected and ensures that a public body's internal policies and procedures that align with POPA.

Key purposes of a PMP include the following:

- Promote accountability by establishing clear roles, responsibilities, and processes for managing privacy risks.
- Foster trust with Albertans, employees, and partners by demonstrating a commitment to privacy.
- Specify safeguards to protect personal information, data derived from personal information and non-personal.
- Enable risk management tools to identify, assess, and mitigate privacy risks proactively.
- Support Business Objectives by integrating privacy into business operations, enabling innovation while respecting individuals' rights.

Requirements

POPA requires public bodies to make reasonable security arrangements to protect the personal information, data derived from personal information and non-personal data. The Protection of Privacy Regulation section 1(c) defines reasonable security arrangements as administrative safeguards, physical safeguards and technical safeguards to protect personal information, data derived from personal information and non-personal data in the custody or under the control of a public body that:

> (i) are appropriate and proportional with the security classification level of the information or data, and
> (ii) in the case of non-personal data, ensure, to the extent possible, that the identity of an individual who is the subject of the non-personal data cannot be re-identified from the data.

Administrative safeguards are a policy, procedure or practice to manage a public body's conduct that protects the privacy of personal information, data derived from personal information and non-personal data;

Physical safeguards are a measure to protect a public body's physical assets, including electronic information systems, from natural and environment hazards and unauthorized intrusion;

Technical safeguards are a measure to protect a public body's electronic information and control access to it.

Implementation

Section 25(5) requires that each public body must implement a PMP within 1 year of enactment of the POPA, and the public body is not required to provide a person with a copy of its PMP or with directions on where to access a copy until 1 year after enactment of the POPA.

PMP Components

A PMP must be proportional to the volume and sensitivity of personal information in the custody or under the control of the public body. Section 6 of the Protection of Privacy (Ministerial) Regulation details the requirements for PMPs.

All public bodies

A designated or identification of a privacy officer

The head of a public body must designate or identify a privacy officer for the public body. This contact is responsible for ensuring the public body's compliance with the POPA. There are times where a head may assign one or more privacy contacts depending on several factors, including the size and structure of the organization.

The privacy officer should be responsible for the development, implementation and maintenance of the PMP, and ensuring the tasks and responsibilities set out in the PMP are incorporated in the organizational structure. Best practices also include reporting back to senior leadership on compliance with POPA and any privacy risks and mitigation strategies.

Internal policies and procedures that address the public body's duties under POPA

Specific policies and procedures need to be developed for the following:

- Responding to requests for the correction of an individual's personal information (see fact sheet on correction of personal information);
- Responding to privacy incidents (see fact sheet on privacy incidents);
- Responding to privacy complaints;
- Creation, use and disclosure of non-personal data, if the public body will create, use or disclose non-personal data (see fact sheets on non-personal data and data matching); and
- How automated systems will use personal information, including any security or technical safeguards and to generate content or make decisions, recommendations.

Establish a security classification system

All public bodies are required to establish a security classification system for personal information, data derived from personal information and non-personal data.

Security classification levels should be reflective of the sensitivity of personal information (see section 2 of the Protection of Privacy (Ministerial) Regulation. The classification should ensure that sensitive information is adequately protected in relation to the context in which the information exists. Security classification systems are required for the application of security and other measures, such as more stringent rules around collection, use and disclosure, to ensure it will be adequately protected.

It is important to effectively manage the information by applying appropriate retention and destruction policies to the information.

Mandatory training for employees

Privacy training and awareness help keep privacy and security top of mind for employees. Training ensures knowledge of policy or legislative requirements and helps prevent and detect privacy incidents or other POPA compliance issues.

Employees in the context of a public body includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body. This means that contractors and other individuals providing a service to a public body are required to be compliant with POPA and understand their responsibilities under the Act. Training requirements ensure these individuals understand their responsibilities.

Timelines for the periodic review

Regular review, assessment and updates to timelines for public bodies to revisit PMPs should be documented. This ensures a public body is monitoring, assessing and revising their PMPs to ensure it remains relevant and effective. Time frames can be developed by the public body based on their size and handling of personal information, data derived from personal information and non-personal data.

Public bodies with high volume of personal information or highly sensitive personal information

Any public body that manages a high volume of personal information or highly sensitive personal information is required to have more components in their PMPs. Public bodies need to exercise their judgement on when a more detailed PMP is required.

Where considering if the public body meets the requirement based on high volume of personal information the public body should take into consideration the size of the public body, the amount of individuals the public body services and the types and amount of personal information the public body has in its custody or under its control.

High-sensitivity information is defined in section 1 of the Protection of Privacy (Ministerial) Regulations to include personal information related to biometric information, financial information, or personal information respecting a minor, senior or vulnerable individual.

These PMPs include additional documentation for their internal privacy management structure and internal policies and procedures.

Documentation of the public body's internal privacy management structure

A public body should ensure roles, responsibilities and accountabilities of employees are clearly documented and ensuring privacy compliance of third-party service providers that handle personal information (contract management, auditing, performance monitoring). This goes beyond just identification of a privacy officer.

One way to achieve this is through implementing delegation matrix that clearly identifies roles and responsibilities under the Act for example responding to complaints on the collection, use and disclosure of personal information, clear authorities for who can release personal information etc. For more information see Fact Sheet: Delegation.

Completing and submitting privacy impact assessments (PIAs)

A public body should establish and create policies and procedures on when PIAs are required to be completed internally to the public body. While POPA requires PIAs to be completed and submitted to the Information and Privacy Commissioner in certain circumstances, these policies should document internal best practices on privacy risk management and what a public body considers a substantial change to an existing administrative practice, program, project or service.

Additionally, as POPA and the accompanying Ministerial Regulation requires submission of the PIA in certain circumstances to the Information and Privacy Commissioner these policies should document who the point of contact is for submitting PIAs to the Commissioner, responsibilities for responding to requests from the Information and Privacy Commissioner for clarification or more detail related to the PIA and following up on any comments or recommendations.

These policies or procedures should also detail how the public body maintain their PIAs.

Proactive monitoring of information systems to assess security measures and mitigate risks

Incorporate privacy risk assessments (e.g., PIAs and Security Threat Risk Assessments), into organizational risk management, and maintain a privacy risk registry. Reporting of these assessments and management of the risks should happen in accordance with requirements of Act and Regulation, and in accordance with the governance structure.

Oral, electronic and written consent

Public bodies should be developing internal policies compliant with section 2 of the Protection of Privacy Regulation that allows the head of the public body to established rules respecting the purposes for which electronic consent, oral and written consent are considered acceptable.

Artificial Intelligence

Public bodies are required to develop policies related to the use of personal information in artificial intelligence systems, the creation of data derived from personal information and the creation of non-personal data, if applicable to the public body.

Safeguards

Public bodies should have policies and procedures that detail administrative, technical and physical safeguards for managing personal information, data derived from personal information and non-personal data. This should

include monitoring the continued integrity of the program, the data life cycle, and the integrity of the information at any time it is used for purposes other than its destruction.

PMP Program Documentation Available Upon Request

Any person may request a copy of a public body's PMP. A public body must provide a copy or provide directions on where to access a copy of the PMP, within 30 business days of the request. A public body may withhold technical information (e.g., security-related information or other information) that could compromise the security of personal information in the custody or under the control.

As a best practice, public bodies may wish to proactive disclose their PMP on their website.

The requirement for a PMP comes into effect one year after the enactment of POPA.

Additional Policies, Processes and Procedures

The Protection of Privacy (Ministerial) Regulation includes the minimum requirements of what a public body PMP should include. Public bodies may wish to expand their PMP to include additional documentation related to other POPA and regulation requirements. This may include:

- establishing processes for human oversight, auditing and validation measures for systems used to create data derived from personal information or non-personal data (as per section 3(2) of the Protection of Privacy (Ministerial) regulation); and
- processes for ensuring accuracy and reliability of data derived from personal information or non-personal data created by the public body (as per section 3(2) of the Protection of Privacy (Ministerial) regulation).

Reference

Protection of Privacy Act

Protection of Privacy Ministerial Regulations

***Protection of Privacy Act* Guide**

Fact Sheet: Privacy Impact Assessments

Fact Sheet: Common or Integrated Program or Service

Fact Sheet: Artificial Intelligence and Automated System