Privacy Management Program Guidance for B.C. Public Bodies

Corporate Information and Records Management Office

December 2022 | Version 1

TABLE OF CONTENTS

INTRODUCTION

Section 36.2 of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires B.C. public bodies to develop a privacy management program (PMP).[1] A PMP is an evolving set of policies, procedures and tools developed by a public body to enable systematic privacy protection throughout the personal information lifecycle.

The Privacy Management Program Directions (PMP Directions), issued by the minister responsible for FOIPPA, describe the mandatory components for PMPs.

Use this guidance to understand the requirements for PMPs. This guidance is for non-ministry public bodies in B.C.

For ministries, the B.C. government follows the Privacy Management and Accountability Policy.

PRIVACY MANAGEMENT PROGRAM COMPONENTS

1. DESIGNATING A PRIVACY CONTACT PERSON

The PMP Directions require that the head of the public body appoint a privacy contact.

The head of the public body may decide to assign more than one privacy contact depending on several factors, including the size and structure of the organization. While many public bodies may opt for a single privacy contact, a public body with multiple locations and/or a large amount of personal information may choose to appoint more than one privacy contact.

POINT OF CONTACT FOR PRIVACY MATTERS

The privacy contact is the point of contact for privacy-related matters such as privacy questions or concerns. The public body may wish to list the individual's contact information on their website and in their communications materials. It may also be helpful to incorporate the contact information and a role description in onboarding materials for new employees.

SUPPORT DEVELOPMENT OF PRIVACY POLICIES AND/OR PROCEDURES

The privacy contact supports the development, implementation, and maintenance of the public body's privacy policies and/or procedures. An example that can be used by public bodies is the B.C. government's Privacy Management and Accountability Policy.

Whether or not a public body already has privacy policies and procedures in place, it could consider conducting a self-assessment to understand where policy gaps may exist or if existing policies and procedures need updating to ensure the public body meets the mandatory PMP components.

Public bodies may want to consider developing policies and procedures on the following topics:

[1] Note that FOIPPA and the corresponding regulation are in the process of being updated to reflect the new requirements.

- Collection notices;
- Consent;
- Accuracy and correction of personal information;
- Permitting individuals to access their own personal information;
- Records retention (and disposal) schedules;
- Reasonable security for the personal information in the public body's custody or under its control;[2] and
- Completing privacy impact assessments (PIAs).

Keep in mind that the PMP policies and procedures can be scaled in proportion to the volume and sensitivity of the personal information in the custody or under the control of the public body.

SUPPORT COMPLIANCE WITH FOIPPA

There are numerous resources available for support:

- The B.C. government's Guide to Good Privacy Practices contains useful information relevant to both government ministries and non-ministry public bodies.
- The Office of the Information and Privacy Commissioner's (OIPC) website has guidance documents for dealing with FOIPPA obligations. Topics range from common privacy concerns to privacy best practices to interpreting FOIPPA requirements.
- The B.C. government's Privacy and Access Helpline (email: privacy.helpline@gov.bc.ca or call 250-356-1851) is available for anyone who has questions related to privacy. This includes ministries, non-ministry public bodies, the private sector, and citizens. While the Privacy and Access Helpline staff cannot provide legal advice, they can provide guidance on privacy-related matters.

Executive support and commitment are also necessary factors in creating a culture of privacy within a public body, which helps support compliance with FOIPPA.

2. PRIVACY IMPACT ASSESSMENTS AND INFORMATION-SHARING AGREEMENTS

The PMP Directions require that a public body has a process in place for completing and documenting Privacy Impact Assessments (PIAs) and Information-Sharing Agreements (ISAs).

PRIVACY IMPACT ASSESSMENTS

A PIA is a step-by-step review process to make sure that a public body is meeting its privacy requirements under FOIPPA and helps a public body identify and mitigate any privacy risks involved in a particular initiative. Section 69 (5.3) of FOIPPA requires that public bodies complete PIAs, and the PMP Directions require a process for completing and documenting PIAs.

[2] For definitions of "custody" and "control," see Schedule 1 of FOIPPA or the FOIPPA Policy and Procedures Manual.

PIAs are typically completed with the help of privacy contacts and the individuals working on the initiative. As noted in the PIA Directions, the goal is to work together to identify, evaluate and manage privacy risks. The PIA Directions also provide guidance on the required elements of a PIA.

For example, the B.C. government has a 5-step PIA review process to complete and document PIAs. There is also a PIA template for non-ministry public bodies that can be used.

INFORMATION-SHARING AGREEMENTS

As defined under section 69 of FOIPPA, an information-sharing agreement (ISA) is an agreement that sets the conditions on the collection, use or disclosure of personal information by the parties to the agreement.

The PMP Directions require public bodies to have a process in place for completing and documenting ISAs as appropriate under FOIPPA. Even if a public body does not expect to initiate ISAs, the process will be helpful if another entity wishes to initiate an ISA with the public body.

The B.C. government has developed guidance for ISAs and a sample ISA template. Public bodies may have other pieces of legislation and/or regulations besides FOIPPA that authorize information sharing. It is recommended that public bodies confirm their legal requirements before adapting the government examples for their specific context.

3. PRIVACY COMPLAINTS AND PRIVACY BREACHES

A privacy breach is the theft or loss of personal information, or the access, collection, use or disclosure of personal information in the custody or control of a public body that is not authorized by FOIPPA. A privacy complaint is a complaint from an individual about a breach of their own personal information.

Note that a privacy breach is not limited to written or recorded information. Personal information that is breached verbally may need to be responded to in the same manner as other breaches.

The PMP Directions require public bodies to have a documented process in place to respond to any privacy breaches and complaints. As an example, the B.C. government has developed an Information Incident Management Policy (IIMP).

As outlined in section 36.3 of FOIPPA, if a privacy breach is reasonably expected to result in significant harm to an individual, public bodies are required to issue a notification about that breach to the affected individual and to the Information and Privacy Commissioner. Refer to the Guidance on Mandatory Privacy Breach Notifications for more information.

A documented breach response process may include the following aspects:

1. Mechanism for employees to immediately report actual or suspected breaches to a supervisor and privacy contact so that the alleged breach can be confirmed and dealt with.
2. Determining the level of harm and the need for breach notification in accordance with the *Freedom of Information and Protection of Privacy Regulation*. Refer to the Guidance on Mandatory Privacy Breach Notifications.

3. Notifying affected individuals and the Information and Privacy Commissioner as required under section 36.3 of FOIPPA.
4. Containment and recovery steps that the public body may take depending on the circumstances. Containment involves preventing further spread of the breached personal information. Recovery involves retrieving the records containing the breached personal information.
5. Mechanisms for investigating the nature, extent and/or cause of the breach.
6. Preventative measures to avoid breaches from occurring in the future. This may include improving security measures.
7. Documentation of breaches and keeping this documentation in accordance with the public body's records retention requirements.[3]
8. Responding to privacy complaints.[4]
9. Administrative fairness practices.[5] Examples of administrative fairness may include ensuring individuals under investigation are aware of the allegations against them and have a fair opportunity to respond to the allegations; and investigators and decisions-makers are free from conflict and are unbiased, and decisions are made based on evidence.

4. PRIVACY AWARENESS AND EDUCATION ACTIVITIES

Privacy training and awareness helps employees identify personal information, understand their privacy obligations, and are an important part of breach prevention.

Awareness and education activities can be scaled based on the volume and sensitivity of the personal information in the public body's custody or control and based on the role of the employee. For example, the privacy obligations of an employee who infrequently handles low sensitivity personal information are different from the employee who often handles sensitive personal information. Therefore, the training and awareness required for those two employees is not necessarily the same.

Education activities should be timely. For example, training should be implemented when there are significant changes to how the public body collects personal information, when systems or processes change, as part of new employee onboarding processes, and periodically to refresh employees' knowledge.

The following privacy topics for education activities are relevant for most public bodies:

- An understanding of what constitutes personal information.
- Appropriate collection, use and disclosure of personal information.
- Reasonable security measures and access controls to protect personal information.

---

[3] Section 31 of FOIPPA requires public bodies retain personal information for at least one year if it is used to make a decision that directly affects an individual.
[4] Privacy complaints may result when an individual has concerns about how a public body handled or processed their personal information.
[5] Fairness in Practice Guide, the Office of the Ombudsperson. In B.C., fairness and good public administration is overseen by the BC Ombudsperson for the broader public sector.

- Identification and reporting of privacy breaches and privacy complaints.

Training on the following topics may also be included:

- Privacy impact assessments.
- Privacy and security requirements for storage of sensitive personal information outside of Canada.

The B.C. government has developed FOIPPA Foundations: Privacy and Access Fundamentals. This course can be used by public bodies when educating their employees and service providers. This free, interactive, online course provides information on privacy and access fundamentals in B.C.

Employees may also benefit from understanding why privacy is important and the underlying principles for privacy protection. The 10 Privacy Principles and Guide to Good Privacy Practices can help with this understanding.

5. MAKING PRIVACY PRACTICES AND POLICIES AVAILABLE

As outlined in the PMP Directions, public bodies are required to make their privacy policies and any documented privacy processes or practices available to employees and, where practicable, to the public.

For employees, this could include adding privacy information to onboarding materials and creating a privacy section on public body internal websites.

Public bodies can decide on the best approach for making these materials available to the public. For example, if the public body has a website, they may wish to publish their privacy policy and related privacy processes or practices online. Smaller public bodies may wish to have their privacy polices on hand in case someone from the public asks to see them. The key is to determine what is practicable for the public body or what the public body is capable of doing to make those policies, processes, or practices available.

In addition, public bodies should consider publishing any privacy awareness and education activities as well as summaries of PIAs and ISAs where appropriate. For example, the B.C. government publishes a summary of PIAs and ISAs through the Personal Information Directory, which documents the management of personal information holdings of government and assists the public in identifying the location of personal information about them held by government.

6. INFORMING SERVICE PROVIDERS OF PRIVACY OBLIGATIONS

When service providers handle personal information related to the provision of services for a public body, the public body must inform them of their privacy obligations.

Contracts are one way to demonstrate privacy obligations for service providers. The B.C. government's privacy protection schedule is an example that can be modified by other public bodies to suit their needs.

PIAs are another useful tool to demonstrate how public bodies and service providers can meet their privacy obligations. By completing a PIA, a public body can assess the services, confirm compliance for

such things as collection, use and disclosure of personal information under FOIPPA, and identify privacy risks.

Privacy training, policies and processes will also support a service provider in complying with their privacy obligations when providing services for a public body.

7. MONITORING AND UPDATING

It is important to review the PMP regularly and ensure it is still relevant to the public body's activities and personal information holdings. For example, this could include an annual review or a review when there is a large change in the public body's operations.

Suggested guiding questions for the review include:

- What are the latest privacy or security threats and risks that the public body needs to be aware of?
- Are the public body's policies and procedures reflecting the latest guidance or complaint and audit findings of the OIPC?
- Are new services being offered that involve increased collection, use or disclosure of personal information? Has the PMP been updated to reflect these new services?
- Is training occurring? Is training effective?
- Are privacy policies and procedures being followed?
- Are contracts with service providers up to date and being followed?

Examples of PMP assessment tools include:

- Privacy Maturity Assessment (Saskatchewan)
- Privacy Program Evaluation (Yukon Ombudsman)
- Privacy Management Program – Gap Analysis for Larger Public Bodies and Municipalities (Nova Scotia)
- Privacy Management Program – Gap Analysis for Smaller Public Bodies & Municipalities (Nova Scotia)
- Accountable Privacy Management in BC's Public Sector (BC OIPC)

These tools and guiding questions can be used to ensure the public body's PMP remains appropriate to their activities and is compliant with FOIPPA.

CONTACT

For questions or comments regarding these guidelines, please contact:

Privacy, Compliance and Training Branch
Corporate Information and Records Management Office
Ministry of Citizens' Services
Telephone: (250) 356-1851
Email: privacy.helpline@gov.bc.ca