Privacy Impact Assessment for Public Bodies

Table of Contents

Use this privacy impact assessment (PIA) template if you work for or are a service provider to the Government of B.C. and are starting a new initiative or significantly changing an existing initiative.

Before you start

- An initiative is an enactment, system, project, program, or activity
- Find PIA templates for initiative update, enactments or broader public sector use
- Contact your Privacy Officer (PO) for help with your PIA
- Find information on the PIA review process and question-by-question guidance
- Protecting privacy involves managing records and providing reasonable security for information throughout its lifecycle. Contact your Records Officer for questions about information management and your Information Security Officer for questions about information security
- If you have any questions, email Privacy.Helpline@gov.bc.ca or phone 250 356-1851

PART 1: GENERAL INFORMATION

Privacy, Compliance and Training Branch (PCT) intake number / PIA file number:

Initiative title:	
Organization:	
Branch or unit:	
Your name and title:	
Your email:	
Initiative Lead name and title:	
Initiative Lead email:	
Privacy Officer:	
PO email:	

Your MPO will complete the questions in the table below.

FOR MPO USE ONLY
Is this a PI or non-PI assessment?
Is this initiative a data-linking program under FOIPPA?
Is this initiative a common or integrated program or activity under FOIPPA?
Related PIAs, if any:
Does this initiative involve disclosures of sensitive personal information outside of Canada?
Provide a brief summary of the initiative to be published in the Personal Information Directory. This summary may be similar to the answer to question 1.

Is there an Information Sharing Agreement as part of this initiative? If yes, please have the Information Sharing Agreement Supplement attached to this PIA when submitting to PCT.

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

3. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose, or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Type "yes" or "no" to indicate your response.

- If yes, go to Part 2

- If no, answer question 4 and submit questions 1 to 4 to your MPO. You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident or privacy breach.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you to identify the legal authority for collecting, using, and disclosing personal information and to confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use, and disclosure

Fill in the first column of this table. Your MPO will identify whether each step represents collection, use, or disclosure and will make sure you have legal authority for what you want to do. Your MPO completes the shaded section of the table. Add or delete rows as needed.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**MPO fills in Collection, use, disclosure**	**MPO fills in FOIPPA authority**	**MPO fills in Other legal authority**
Step 1:			
Step 2:			
Step 3:			
Step 4:			

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

6. Collection Notice

If you are collecting personal information directly from the individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Review the sample collection notice and write your collection notice below. You can also attach the notice as an appendix.

FOR MPO USE ONLY
If applicable, list the exception to a collection notice.

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

Type "yes" or "no" to indicate your response.

- If yes, go to question 8
- If no, go to Part 5

8. Where are you storing the personal information involved in your initiative?

9. Does your initiative involve sensitive personal information?

Type "yes" or "no" to indicate your response.

- If yes, go to question 10
- If no, go to Part 5

10. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

Type "yes" or "no" to indicate your response.

- If yes, go to Part 5

- If no, contact your MPO and go to Part 4

PART 4: ASSESSMENT OF DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You will likely need your MPO's help to complete this section. More help is available in the Guidance on Disclosures Outside of Canada.

11. Is the sensitive personal information stored by a service provider?

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	**Name of cloud infrastructure and/or platform provider(s) (if applicable)**	**Where and how is the sensitive personal information stored (including backups)?**

12. Provide details on the disclosure, including to whom it is disclosed and where and how the sensitive personal information is stored.

13. Describe the contractual terms in place (if applicable).

If you wish to modify the Privacy Protection Schedule, email Privacy.Helpline@gov.bc.ca or call 250 356-1851 for approval.

For example, indicate if you have attached the Privacy Protection Schedule.

14. Are you relying on an existing contract, such as an enterprise offering from the Office of the Chief Information Officer (OCIO)?

Type “yes” or “no” to indicate your response.

- If yes, go to question 14.1
- If no, go to question 15

14.1 Which enterprise service are you accessing?

There may be a corporate PIA or other information to help you.

15. What controls are in place to prevent unauthorized access to sensitive personal information?

16. Provide details about how you will track access to sensitive personal information.

17. Describe the privacy risks for disclosure outside of Canada.

Use the table below to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high)**	**Risk response (this may include contractual mitigations, technical controls and/or procedural and policy barriers)**	**Is there any outstanding risk? If yes, please describe.**

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the organization on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17.

PART 5: SECURITY OF PERSONAL INFORMATION

This part captures information about the privacy aspects of securing personal information. People, organizations, or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical (e.g., your office building or work environment) and technical (e.g., online cloud service) environments.

18. Does your initiative involve digital tools, databases or information systems?

Type "yes" or "no" to indicate your response.

- If yes, you may need to involve your PO and possibly your Information Security Officer (MISO). Together you can assess whether your initiative needs a security assessment

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the reasonable security requirements of FOIPPA section 30?

Type "yes" or "no" to indicate your response.

- If you answered yes to questions 18 and 18.1, skip question 19 and go to question 20

19. Are all digital records stored on government servers and are all physical records stored in government offices with government security?

Type "yes" or "no" to indicate your response. If yes, go to question 20

- If no, describe where the records are stored and the technical and physical security measures in place to protect those records.

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We allow employees only in certain roles access to information	
Employees that need standing or recurring access to personal information must be approved by the appropriate authority	
We use audit logs to see who accesses a file and when	
Describe any additional strategies:	

PART 6: ACCURACY, CORRECTION, AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 Do you have a process in place to correct personal information?

Type "yes" or "no" to indicate your response.

22.2 Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Will you document the request to correct or annotate the record?

Type "yes" or "no" to indicate your response.

22.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party recipient of the request for correction. Will you ensure that you conduct these notifications when necessary?

Type "yes" or "no" to indicate your response.

23. Does your initiative use personal information to make decisions that directly affect an individual?

Type "yes" or "no" to indicate your response.

- If yes, go to question 24
- If no, skip ahead to Part 7

24. Do you have an approved information schedule in place related to personal information used to make decisions?

FOIPPA requires that ministries keep personal information for a minimum of one year after it is used to make a decision about an individual. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule or with the approval of the Chief Records Officer.

Type "yes" or "no" to indicate your response.

If you answered no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

PART 7: PERSONAL INFORMATION BANKS

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

25. Will your initiative result in a personal information bank?

Type "yes" or "no" to indicate your response.

- If yes, please complete the table below.

Describe the type of information in the bank
Name of agency involved
Any other ministries, agencies, public bodies, or organizations involved
Business contact title and phone number for person responsible for managing the Personal Information Bank

PART 8: ADDITIONAL RISKS

26. In the table below describe any additional risks that arise from collecting, using, disclosing, or storing personal information in your initiative that have not been addressed by the questions on the template.

Add new rows if necessary.

Possible risk	**Response**
Risk 1:	
Risk 2:	
Risk 3:	

PART 9: SIGNATURES

You have completed a Privacy Impact Assessment. PCT will review, comment and sign this document first before returning it to your program area for signatures.

PCT will review the PIA and create a summary of the review.

PCT Summary

This section summarizes PCT's review of the PIA and identifies decisions made that are not otherwise noted.

PCT Comments:

PCT Signatures

This PIA is based on a review of the material provided to PCT as of the date below.

Role	Name	Electronic signature	Date signed
PCT Privacy Advisor			
PCT Manager or Director Only required if personal information is involved			

Signatures

This PIA accurately documents the data elements, information flow, and information about disclosure and storage outside of Canada at the time of signing. If there are any significant changes to the overall initiative, including to the way personal information is collected, used, stored, or disclosed, the program area will engage with their MPO and if necessary, complete a PIA update to submit to PCT. You may choose to add signatories.

Please ensure that you have reviewed the privacy risks and risk responses in Part 4: Assessment of Disclosures Outside of Canada.

Comments

Role	Name	Electronic signature	Date signed
Initiative Lead			
Executive Lead or designate Only required if personal information is involved			

	Name	Electronic signature	Date signed
Privacy Officer (PO)			
Information Security Officer Only required if ISO was involved in conducting the PIA			