Office of the Information and Privacy Commissioner of Alberta

PROTECTION OF PRIVACY ACT (POPA) BREACH NOTIFICATION ASSESSMENT TOOL

Section 10(2)(b) of the *Protection of Privacy Act* and Section 4(4) of the *Protection of Privacy (Ministerial) Regulation*

Disclaimer:

This document is not intended as, nor is it a substitute for, legal advice, and is not binding on the Information and Privacy Commissioner of Alberta. Responsibility for compliance with the law (and any applicable professional or trade standards or requirements) remains with each organization, custodian or public body. All examples used are provided as illustrations. The official versions of the laws the OIPC oversees and their associated regulations should be consulted for the exact wording and for all purposes of interpreting and applying the legislation. The Acts are available on the website of Alberta King's Printer.

June 2025

Introduction

This tool is designed to assist public bodies, as defined in the *Protection of Privacy Act* (POPA) to assess whether **they are required** to notify individuals, the Commissioner, and the Minister following the loss of, unauthorized access to or unauthorized disclosure of personal information in their custody or under their control.

Public bodies are **required** to notify affected individuals, the Commissioner, and the Minister following the loss of, unauthorized access to or unauthorized disclosure of personal information in their custody or under their control, where a reasonable person would consider that **there exists a real risk of significant harm (RROSH)** to an individual as a result of the loss of, unauthorized access to or unauthorized disclosure of personal information (section 10(2) of POPA).

THIS ASSESSMENT TOOL IS NOT FOR CUSTODIANS OR ORGANIZATIONS

Custodians as defined in the *Health Information Act* (HIA) and Organizations as defined in the *Personal Information Protection Act* (PIPA), have different breach notification obligations, and must use the appropriate breach notification assessment tools available on the OIPC website.

If at any stage of the assessment you are unsure on how to proceed or have questions, please contact the Office of the Information and Privacy Commissioner (OIPC) at **780-422-6860 or 1-888-878-4044 (toll free) or by email at generalinfo@oipc.ab.ca**.

For each question, click on the box (☐) to check or uncheck the box.

Public bodies are not required to submit a copy of this assessment to the Commissioner upon completion of the assessment.

1. Are you a public body as defined by section 1(u) of *POPA?*

A public body means a department, branch or office of the Government of Alberta; an agency, board, commission, corporation, office or other body designated as a public body in the regulations; the Executive Council Office; the office of a member of the Executive Council; the Legislative Assembly Office, the office of the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner, the Information and Privacy Commissioner, the Child and Youth Advocate or the Public Interest Commissioner; or a local public body pursuant to section 1(u) of POPA).

☐ Yes *(proceed to question 2).*
☐ No ***(STOP – you are not required to provide notification of a breach under POPA).***
☐ Unsure **(STOP –** *You may contact the OIPC if you have questions.*)

2. Is personal information as defined in section 1(q) of POPA involved?

Personal information means recorded information about an identifiable individual, ***including*** *the individual's name, home or business address, home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal in the individual's capacity as an employee or agent, the individual's race, national or ethnic origin, colour or religious or political beliefs or associations, the individual's age, gender identity, sex, sexual orientation, marital status or family status, an identifying number, symbol or other particular assigned to the individual, the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics, information about the individual's health and health care history, including information about the individual's physical or mental health, information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given, anyone else's opinions about the individual, and the individual's personal views or opinions, except if they are about someone else - section 1(q) of POPA.*

☐ Yes *(proceed to question 3).*
☐ No **(STOP -** ***you are not required to provide notification of a breach under POPA*****)**
☐ Unsure **(STOP –** *You may contact the OIPC if you have questions.)*

3. Which of the following incidents affected the personal information in question 2?

In this document, an incident means an occurrence or a situation involving the loss of, unauthorized access to or unauthorized disclosure of personal information. See appendix below for some examples of incidents that can affect personal information.

(select all that apply)

☐Loss of the personal information *(proceed to question 4)*

☐Unauthorized access to the personal information *(proceed to question 4)*

☐Unauthorized disclosure of the personal information *(proceed to question 4)*

☐None of the above **(STOP - *you are not required to provide notification of a breach under POPA*)**

☐Unsure **(STOP -** *You may contact the OIPC if you have questions.)*

4. At the time of the incident identified in question 3, was the personal information in the custody or under the control of the public body in question?

In paragraph 39 of Order F2016-64, "custody or control" refers to an enforceable right of an entity to possess a record or to obtain or demand it, if the record is not in its immediate possession. "Custody or control" also imparts the notion that a public body has duties and rights in relation to a record, such as the duty to preserve or maintain records, or the right to destroy them. [See the appendix of this document]. As an example, information is in the custody and control of a public body if the information is stored on a server or file cabinet owned by the public body in the public body's premises. If a public body contracts a storage company to store personal information on behalf of the public body or uses a cloud provider, the public body does not have physical custody of the information but maintains control over the information by virtue of an agreement with the storage or cloud provider.

⭘Yes *(proceed to question 5)*

⭘No **(STOP** – *the public body must have had custody or control of the information at the time of the incident identified in question 3.)*

⭘Unsure (**STOP –** *You may contact the OIPC if you have questions.*)

5. Has the public body conducted an assessment of harm to an individual who is the subject of the information that has been lost, accessed or disclosed without authorization?

Public bodies should have an established process in place for assessing the existence of harms and for determining if such harms are significant to an individual as a result of the loss of, unauthorized access or unauthorized disclosure. Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identify theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property or other legal harms or financial losses.

⭘Yes *(proceed to question 6)*

⭘No **(STOP –** *Complete an assessment of significant harm before proceeding.)*

6. Has the public body performed an assessment of the RROSH to individuals who are the subjects of the information involved in the loss or unauthorized access to or unauthorized disclosure?

Public bodies must assess RROSH to an individual following a loss of, unauthorized access to or unauthorized disclosure of personal information of the individual. In assessing RROSH, public bodies must consider the factors set out in sections 4(1) and (2) of the Protection of Privacy (Ministerial) Regulation (M-Regulation). See appendix below for prescribed requirements for RROSH assessment.

☐ Yes *(proceed to question 7)*
☐ No (**STOP –** *sections 4(1) and (2) of the M-Regulation requires the public body to conduct a RROSH assessment.*)

7. What is the public body's assessment of RROSH to an individual who is the subject of the information that has been lost, accessed or disclosed without authorization?

The RROSH assessment must be conducted in relation to the individuals who are the subjects of the personal information that is lost, accessed or disclosed without authorization, considering the factors listed in sections 4(1) and (2) of the M-Regulation. For instance, the M-Regulation requires the public body to consider the sensitivity of the personal information that was lost, accessed or disclosed without authorization, and any mitigating measures taken or other factors that reduce the RROSH etc.

☐ There exists a real risk of significant harm ***(The public body is required to notify the individuals affected, the Commissioner, and the Minister in writing in accordance with sections 4(3) (4) and (5)) of the M-Regulation.)***
☐ There is no real risk of significant harm *(The public body is not required to notify the affected individual, the Commissioner and the Minister.)*

Based on the result of the assessment, if you are required to notify, complete the POPA Breach Notification Form

Name of Public Body	
Public Body's file # (if applicable)	
Date of Assessment	
Date of discovery	
Breach Description	

Appendix

Examples of common privacy breaches

Privacy breaches occur in a number of ways. Human error and malicious actions by threat actors can cause privacy breaches. A cybersecurity incident such as a ransomware or phishing attack may lead to privacy breaches if personal information is lost, accessed or disclosed as a result of the incident. Some common privacy breaches that have been reported to the Commissioner include:

- Loss or theft of unencrypted mobile devices (e.g. laptops, USB sticks or hard drives) containing personal information.
- Misdirected communications (via email, fax or mail) containing personal information.
- Snooping of (unauthorized access to) patient or customer records by employees (authorized users).
- Ransomware attacks resulting in exfiltration of personal information from a computer system and/or the encryption of the information within the compromised systems thereby preventing authorized users from accessing the information.
- Insecurely disposing of paper records containing personal information by putting the records in a dumpster.
- Disposing of computer systems or storage media without first securely removing personal information stored in them.
- Stolen paper records containing personal information following a break-in into an office, employee's vehicle or a storage facility.
- Break-in into a record storage facility where paper records containing personal information may not be stolen but accessed by the unauthorized individuals.
- Inadvertent exposure of personal information over the internet due to system misconfiguration.

Custody or Control

- OIPC Order F2016-64 issued by the OIPC, sets out the criteria for determining whether a public body has custody or control:

  [Para 40] Previous orders of this office have considered a non-exhaustive list of factors compiled from previous orders of this office and across Canada when answering the question of whether a public body has custody or control of a record. In Order F2008-023, following previous orders of this office, the Adjudicator set out and considered the following factors to determine whether a public body had custody or control over records:

  - Was the record created by an officer or employee of the public body?
  - What use did the creator intend to make of the record?
  - Does the public body have possession of the record either because it has been voluntarily provided by the creator or pursuant to a mandatory statutory or employment requirement?
  - If the public body does not have possession of the record, is it being held by an officer or employee of the public body for the purposes of his or her duties as an officer or employee?
  - Does the public body have a right to possession of the record?

- Does the content of the record relate to the public body's mandate and functions?
- Does the public body have the authority to regulate the record's use?
- To what extent has the record been relied upon by the public body?
- How closely is the record integrated with other records held by the public body?
- Does the public body have the authority to dispose of the record?

[para 41] Not every factor is determinative, or relevant, to the issues of custody or control in a given case. Custody or control may be determined by the presence of only one factor. If it can be said, after consideration of the factors, that a public body has an enforceable right to possess records or obtain or demand them from someone else, and has duties in relation to them, such as preserving them, it follows that the public body would have control or custody over the records.

Assessment of RROSH

The RROSH assessment is a reasonable person test. This means what a reasonable person would think is appropriate in the situation i.e. where a reasonable person would consider that there exists a RROSH to an individual as a result of the loss, unauthorized access to or unauthorized disclosure of personal information.

Sections 4(1) and (2) of the M-Regulation sets out criteria for assessing RROSH.

> **4(1)** In assessing under section 10(2) of the Act whether there exists a real risk of significant harm to an individual as a result of the loss of, unauthorized access to or unauthorized disclosure of personal information, a public body must consider each of the following factors, in addition to any other relevant factors;
>
> (a) whether there is a reasonable bias to believe that the personal information has been misused;
>
> (b) whether the loss of, authorized access to or unauthorized disclosure of the personal information occurred as a result of malicious intent;
>
> (c) the sensitivity of the personal information that was lost or accessed or disclosed without authorization;
>
> (d) mitigating measures taken or other factors that reduce the risk of significant harm.
>
> **(2)** For the purposes of subsection (1), "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identify theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property or other legal harms or financial losses.

In assessing whether there exists a real risk of significant harm to an affected individual of a breach, public bodies must consider all circumstances surrounding the breach including the following:

- What is the nature of the information involved?
- Is the information sensitive?[1]
- Who obtained or could have obtained access to the information?
- How many persons was the information exposed to?
- Is there any personal or professional relationship between the affected individual and the unauthorized recipient of the information?
- Were there reasonable security controls in place such as encryption to prevent unauthorized access to the information at the time of the breach?
- Did existing security controls in place at the time of the breach have known flaws or vulnerability?
- How long was the information exposed to unauthorized individuals?
- Is there evidence of malicious intent associated with the breach such as theft, hacking or malware attack?
- Could the information be used for criminal purposes such as for identity theft or fraud?
- Was the information recovered if it was lost?
- How many individuals are affected by the breach?
- Are there vulnerable individuals involved such as youth or seniors? Financial information or personal information respecting vulnerable individuals, seniors or minors is considered to be highly sensitive information.
- Can the information be used for targeted attacks such as phishing attack?

Mitigating Factors

Some mitigating factors that may lead to NO RROSH include:

- A stolen mobile device containing personal information was encrypted with an industry standard cryptographic algorithm and the encryption key had not been stolen with the device.
- A stolen mobile device containing personal information was remotely wiped prior to it being accessed.
- A misdirected communication, email or fax, containing personal information was reported by the individual who received the communication in error. In addition, the individual confirmed that the information has been destroyed and has not been disclosed further.
- Personal information that was lost was recovered or returned and there was no malicious intent involved. For instance, a flash drive containing personal information was lost and later recovered and there is evidence that the personal information contained in the flash drive was not accessed.

[1] Sensitive personal information may include but is not limited to biometric information, medical information, banking information, ethnicity, race-based information, Social Insurance Number (SIN), passport information, driver's licence information, child custody information, tax information, etc.