AP I2 Privacy Impact Assessments

Legislative References: *Freedom of Information and Protection of Privacy Act (FOIPPA)* section 69
Policy Reference: None
Collective Agreement References: None
Date: April 25, 2023

Purpose

Section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) requires districts to conduct Privacy impact Assessments (PIA) to determine whether a project involves personal information and if so, how personal information will be protected as it is collected or used in a project.

The purpose of this Administrative Practice is to set out the District's process for conducting a Privacy Impact Assessment in accordance with the FOIPPA. If a new initiative has an application or software associated with its use or implementation, then a New Application/Software Request must first be undertaken and approved in accordance with Administrative Practice I7 New Application/Software Request.

Definitions

"common or integrated program or activity" has the same meaning as in the Act;

"**data-linking program"** has the same meaning as in the Act;

"head" has the same meaning as the head of a public body that is a not a ministry in Schedule 1 of the Act;

"initiative" means an enactment, system, project, program, or activity;

"ministry" means a ministry of the government of British Columbia;

"personal information" has the same meaning as in the Act;

"privacy impact assessment (PIA)" has the same meaning as in the Act;

"privacy risk" includes:

- an inherent risk of unauthorized collection, use, disclosure, or storage of personal information; and
- something that may inappropriately override or otherwise limit personal privacy.

The level of risk may vary based on:

- the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information; and,
- the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information.

"public body" means a public body as defined in the Act that is not a ministry; and,

"service provider" has the same meaning as in the Act.

1. When to Conduct a PIA

1.1. A PIA must be conducted on a new initiative for which no PIA has previously been conducted.

1.2. A PIA must be conducted before implementing a significant change to an existing initiative, including but not limited to a change to the location in which sensitive personal information is stored, when it is stored outside of Canada.

1.3. Where a PIA is not required by items 1.1and 1.2 above, a PIA may be conducted at the discretion of the head, and in accordance with these directions.

2. Elements within a PIA

2.1. Identify the purpose or objective of the initiative.

2.2. Identify the information elements, including personal information, to be collected, used, disclosed, or stored, and confirm that the personal information elements are necessary for the purpose of the initiative.

2.3. Where applicable, identify:

- 2.3.1. how and from whom the personal information will be collected;
- 2.3.2. how the personal information will be used;
- 2.3.3. how and to whom personal information will be disclosed; and
- 2.3.4. if an assessment or disclosure for storage of personal information outside of Canada is required, as per section 3 below..

2.4. Identify relevant legal authority (or authorities) authorizing the collection, use, or disclosure of personal information, as applicable.

2.5. If the initiative involves personal information, identify privacy risks and privacy risk responses that are proportionate to the identified risk.

2.6. Identify reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made.

2.7. Designation of the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative.

2.8. Identify if a supplementary assessment in section 5 of disclosure for storage of personal information outside of Canada is required for an initiative by determining:
  2.8.1. whether the initiative involves personal information that is sensitive; and,
  2.8.2. if the personal information that is sensitive is disclosed to be stored outside of Canada.

3. Where applicable, the head of the public body must confirm their adherence in the PIA to the following requirements under Part 3 of the Act:

3.1. Confirm that notice of collection will be given to individuals per section 27 (2) of the Act, or confirm that notice of collection is not required, per section 27 (3) of the Act;

3.2. Where personal information is used to make a decision that directly affects an individual, confirm that reasonable efforts will be made to ensure the accuracy and completeness of personal information per section 28 of the Act;

3.3. Confirm that a process is in place, per section 29 of the Act, to correct individuals' personal information upon request, or to annotate their personal information if it is not corrected per the individual's request;

3.4. Where personal information is used to make a decision that directly affects an individual, confirm that the personal information will be retained for at least one year after use, per section 31 of the Act;

4. Privacy Assessment Forms

4.1. The district Privacy Assessment Form, in accordance with the template provided by the Minister responsible for the Act, as appended, must be used for a PIA.

5. Directions on a supplementary assessment of disclosure for storage of personal information outside Canada

5.1. If the conditions in 2.8 are not met, or the disclosure outside of Canada is made in accordance with section 33 (2) (f), an assessment of disclosure for storage of personal information outside of Canada is not required.

5.2. If both conditions in 2.8 are met, then an assessment of disclosure for storage of personal information outside of Canada is required.

5.3. If an assessment of disclosure for storage of personal information outside of Canada is required, the head of a public body must identify the privacy risk(s) as well as the level of the privacy risk(s) associated with the disclosure by examining factors which include but are not limited to the following:

- 5.3.1. the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information;
- 5.3.2. the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information;
- 5.3.3. whether the personal information is stored by a service provider; and,
- 5.3.4. where the personal information is stored.

5.4. For each privacy risk, identify a privacy risk response that is proportionate to the level of risk posed. These may include technical, security, administrative or contractual measures (e.g. ways to manage and review access to personal information).

5.5. The outcome of the assessment of disclosure for storage of personal information outside Canada will be a risk-based decision made by the head of the public body on whether to proceed with the initiative, considering 5.3 and 5.4.