



PRIVACY IMPACT ASSESSMENT DIRECTIONS

TO: HEADS OF ALL PUBLIC BODIES THAT ARE NOT
MINISTRIES

DIRECTION: 2-21

SUBJECT: Directions to heads of public bodies that are not ministries on
conducting privacy impact assessments

AUTHORITY: These directions are issued under section 69 (5.3) of the *Freedom
of Information and Protection of Privacy Act*.

APPLICATION: These directions apply to heads of all public bodies that are not
ministries.

EFFECTIVE DATE: November 26, 2021

A handwritten signature in black ink, appearing to read "Lisa Beare", written over a horizontal line.

Honourable Lisa Beare
Minister of Citizens' Services

Minister of Citizens' Services

Directions to Heads of Public Bodies that are Not Ministries issued under Section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*

I, Lisa Beare, Minister of Citizens' Services (the Minister), issue the following directions to heads of public bodies that are not ministries, hereafter referred to as "public bodies", under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 (the Act).

These directions repeal and replace Direction 1/14 issued May 9, 2014.

A. Preamble

Relevant Legislative Requirements

Section 69 (5.3) of the Act requires the head of a ministry to conduct a privacy impact assessment (PIA) and must do so in accordance with the directions of the Minister responsible for the Act.

Purpose

The purpose of these directions is to:

1. Direct public bodies in determining when a PIA must or may be conducted.
2. Direct public bodies in conducting and documenting a PIA that will:
 - a. Determine whether their initiative meets or will meet the requirements under Part 3 of the Act; and
 - b. Identify and assess privacy risks and identify a risk response(s) that is proportionate to the level of the risk.

B. Definitions

In these directions:

“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 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.

C. When a PIA must or may be conducted

1. A head of a public body must conduct a PIA on a new initiative for which no PIA has previously been conducted.
2. A head of a public body must conduct a PIA 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.

3. Where a head of a public body is not required to conduct a PIA by items 1-2, above, they may conduct a PIA at their discretion and in accordance with these directions.

D. General Directions on conducting a PIA

When conducting a PIA for an initiative, the head of a public body must do the following:

1. Identify the purpose or objective of the initiative.
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.
3. Where applicable identify:
 - a. how and from whom the personal information will be collected;
 - b. how the personal information will be used;
 - c. how and to whom personal information will be disclosed; and
 - d. if an assessment or disclosure for storage of personal information outside of Canada is required, as per E.
4. Identify relevant legal authority (or authorities) authorizing the collection, use, or disclosure of personal information, as applicable.
5. If the initiative involves personal information, identify privacy risks and privacy risk responses that are proportionate to the identified risk.
6. Identify reasonable security arrangements against such risks as unauthorized collection, use, disclosure, or storage that have been or will be made.
7. The head of a public body may document the PIA using a template created by the Minister responsible for the Act or an appropriate format as determined by the head of the public body.
8. Designate 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.

9. In addition to the requirements outlined in Directions D1 to D8, identify if a supplementary assessment (E1 to E5) of disclosure for storage of personal information outside of Canada is required for an initiative by determining:
 - a. whether the initiative involves personal information that is sensitive; and,
 - b. if the personal information that is sensitive is disclosed to be stored outside of Canada.

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:

10. 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;
11. 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;
12. 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;
13. 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;

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

1. If the conditions in D9 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.
2. If both conditions in D9 are met, then an assessment of disclosure for storage of personal information outside of Canada is required.
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:

- a. the likelihood of occurrence of an unauthorized collection, use, disclosure, or storage of personal information;
 - b. the impact to an individual(s) of an unauthorized collection, use, disclosure, or storage of personal information;
 - c. whether the personal information is stored by a service provider; and,
 - d. where the personal information is stored.
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. 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 E3 and E4.