



PRIVACY IMPACT ASSESSMENT DIRECTIONS

TO: HEADS OF PUBLIC BODIES THAT ARE NOT
GOVERNMENT MINISTRIES

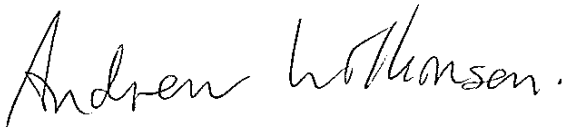
DIRECTION: 2/14

SUBJECT: Directions to heads of Public Bodies that are not government
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 Public Bodies that are not
government ministries.

EFFECTIVE DATE: May 9, 2014



Honourable Andrew Wilkinson
Minister of Technology, Innovation and Citizens' Services

Minister of Technology, Innovation and Citizens' Services

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

I, Andrew Wilkinson, Minister of Technology, Innovation and Citizens' Services, issue the following directions to heads of Public Bodies that are not government ministries under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996 c. 165:

A. Definitions

For the purposes of these directions:

“Common or Integrated Program or Activity” means a program or activity that

- a. provides one or more services through
 - i. a Public Body and one or more other Public Bodies or agencies working collaboratively, or
 - ii. one Public Body working on behalf of one or more other Public Bodies or agencies, and
- b. is confirmed by regulation as being a Common or Integrated Program or Activity.

“Data Linking” means the linking or combining of Personal Information in one database with Personal Information in one or more other databases if the purpose of the linking or combining is different from

- a. the purpose for which the information in each database was originally obtained or compiled, and
- b. every purpose that is consistent with each purpose referred to in paragraph a.

“Data-Linking Initiative” means a new or newly revised system, project, program or activity that has, as a component, Data Linking between

- a. two or more Public Bodies, or
- b. one or more Public Bodies and one or more agencies.

“Employee”, in relation to a Public Body, includes:

- a. a volunteer, and
- b. a service provider.

“Information Sharing Agreement (ISA)” means an agreement between a public body and one or more of the following:

- a. another Public Body;
- b. a government institution subject to the *Privacy Act* (Canada);
- c. an organization subject to the *Personal Information Protection Act* or the *Personal Information Protection and Electronic Documents Act* (Canada);
- d. a public body, government institution or institution as defined in applicable provincial legislation having the same effect as this Act;
- e. a person or a group of persons;
- f. a prescribed entity

that sets conditions on the collection, use or disclosure of Personal Information by the parties to the agreement.

“Personal Information” means recorded information about an identifiable individual other than contact information.

“Personal Information Bank (PIB)” means a collection of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

“Privacy Impact Assessment (PIA)” means an assessment that is conducted by a Public Body to determine if a current or proposed system, project, program or activity meets or will meet the requirements of Part 3 of the *Freedom of Information and Protection of Privacy Act*.

“Privacy Risk” means something that could cause the unauthorized access, collection, use, disclosure, or storage of Personal Information.

“Public Body” means

- a. a ministry of the government of British Columbia,
- b. an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2 of the *Freedom of Information and Protection of Privacy Act*, or
- c. a local public body

but does not include

- d. the office of a person who is a member or officer of the Legislative Assembly, or
- e. the Court of Appeal, Supreme Court or Provincial Court

B. General Directions

Under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, heads of Public Bodies that are not government ministries are directed to:

1. conduct any PIA in accordance with sections B and C of these directions;
2. ensure that a PIA is signed by individuals with primary responsibility for privacy and, where relevant, security.

C. Directions on Conducting a PIA

Under section 69 (5.3) of the *Freedom of Information and Protection of Privacy Act*, heads of Public Bodies that are not government ministries are directed to include the following elements, where applicable, in any PIA conducted:

1. a detailed description of the system, project, program or activity covered by the PIA;
2. a list of the elements of information including Personal Information included in the system, project, program or activity;
3. identification of any information including Personal Information involved in the system, project, program or activity that can be accessed from and/or stored outside Canada;
4. identification of whether the system, project, program or activity involves Data Linking;
5. identification of whether the system, project, program or activity involves a Common or Integrated Program or Activity;
6. an information flow diagram and/or Personal Information flow table that shows how the system, project, program or activity does, or will, collect, use, and/or disclose Personal

Information, including the authorities for the collection, use, and disclosure of Personal Information under the Freedom of Information and Protection of Privacy Act;

- i. an information flow diagram must be included if the system, project, program or activity is related to a Common or Integrated Program or Activity or a Data-Linking Initiative;
7. identification of the Privacy Risks within the system, project, program or activity and for each Privacy Risk identified:
 - i. an explanation of the likelihood of the Privacy Risk occurring;
 - ii. an explanation of the degree of impact the Privacy Risk would have on an individual if it occurred; and
 - iii. a record of the mitigations that have been, or will be, implemented;
8. a description of the physical security measures related to the system, project, program or activity;
9. a description of the technical security measures related to the system, project, program or activity;
10. a description of any specific policies and procedures within the Public Body governing an Employee's management of Personal Information;
11. with respect to technical systems, details of access to Personal Information including as applicable, but not limited to:
 - i. a description of the permissions governing access to the Personal Information;
 - ii. a description of how access to Personal Information is, or will be, tracked; and
 - iii. a description of any access controls and/or ways in which unauthorized changes to Personal Information is, or will be, limited or restricted;
12. an explanation of how the accuracy of an individual's Personal Information is, or will be, ensured;
13. an explanation of how an individual's Personal Information is, or will be, corrected upon their request or an explanation of how an individual's Personal Information is, or will be, annotated if it is not corrected as per the individual's request;

14. with respect to Personal Information, an explanation of the retention and disposition measures that relate to the secure retention and disposition of Personal Information;
15. with respect to Personal Information that is used to make a decision that directly affects an individual, an explanation of how any applicable retention and disposition requirements are, or will be, met;
16. an explanation of any systematic disclosures or regular exchanges of Personal Information included in the system, project, program or activity and reference to any applicable ISA(s);
17. for research that is not out of scope of the *Freedom of Information and Protection of Privacy Act*, as per section 3 (1) (e) of that Act, identification of whether the system, project, program or activity does, or will, involve access to Personal Information for research or statistical purposes and reference to the research agreement, as required under section 35 (1) (d) of the *Freedom of Information and Protection of Privacy Act*; and
18. identification of whether the system, project, program or activity does, or will, involve a PIB and, where applicable, the PIB summary information required under section 69 (6) of the *Freedom of Information and Protection of Privacy Act* for inclusion in a public directory.