Privacy Impact Assessments

Introduction

A Privacy Impact Assessment (PIA) is a systematic process that identifies and evaluates, from the perspective of all stakeholders, the potential effects on privacy of a project, initiative, or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts (Roger Clarke, *Privacy impact assessment: Its origins and development*).

The *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) defines a privacy impact assessment in section 2(w) as "… an assessment that is conducted by a public body as defined under subparagraph (x)(i) to determine if a current or proposed program or service meets or will meet the requirements of Part III of this Act."

In general, it is best practice to conduct a preliminary PIA (PPIA) prior to starting a full PIA; the information contained in the PPIA may lead to the need for a full PIA report. The Government of Newfoundland and Labrador has developed a PPIA checklist for this purpose.

PIAs and the *ATIPPA, 2015*

Recent changes to the *ATIPPA, 2015* require departments and the executive branch of government to complete a privacy impact assessment or a preliminary privacy impact assessment during the development of a program or service. Further, if the PIA involves a common or integrated program or service, the minister must notify the Office of the Information and Privacy Commissioner (OIPC) regarding this program at an early stage of development. Once a PIA in relation to a common or integrated program or service is developed, it must be submitted to the OIPC for the Commissioner's review and comment.

Section 72 (privacy impact assessment) states:

> *72.(1) A minister shall, during the development of a program or service by a department or branch of the executive government of the province, submit to the minister responsible for this Act (a) a privacy impact assessment for that minister's review and comment; or*
>
> *(b) the results of a preliminary assessment showing that a privacy impact assessment of the program or service is not required.*
>
> *(2) A minister shall conduct a preliminary assessment and, where required, a privacy impact assessment in accordance with the directions of the minister responsible for this Act.*

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

> *(3) A minister shall notify the commissioner of a common or integrated program or service at an early stage of developing the program or service.*
>
> *(4) Where the minister responsible for this Act receives a privacy impact assessment respecting a common or integrated program or service for which disclosure of personal information may be permitted under paragraph 68(1)(u), the minister shall, during the development of the program or service, submit the privacy impact assessment to the commissioner for the commissioner's review and comment.*

While not all public bodies are required to conduct PPIAs and PIAs, it is good practice. In addition, while it is not required that the OIPC review all PIAs, this Office would welcome the opportunity to review and provide comments on any PIA that is conducted by a public body.

Further, section 95 of the *ATIPPA, 2015* establishes the general powers and duties of the Commissioner. Departments and branches of the executive government of this Province should be aware that this Office has the authority to conduct investigations to ensure compliance with the *ATIPPA, 2015* and to monitor and audit practices and procedures employed in carrying our responsibilities and duties under the *ATIPPA*, *2015*. Where appropriate, the PIA process would be part of such investigations and audits, as it should help to demonstrate how a public body planned or intended to address identified risks.

What is a Common or Integrated Program or Service?

As the *ATIPPA, 2015* does not define a common or integrated program or service, the OIPC is adopting a definition similar to the one in Schedule 1 of British Columbia's *Freedom of Information and Protection of Privacy Act*. Our definition is:

> *"common or integrated program or service" means a program or service 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*

Please note that the involvement of the Office of the Chief Information Officer (OCIO) does not automatically make a project a common or integrated program or service. For example, if the OCIO is developing an IT system on behalf of a public body, the project would not necessarily fall under this definition.

Early Notice

The Minister must notify the OIPC of a common or integrated program or service when a project is in the conceptual stage. The notice should be provided by letter from the Minister to the OIPC and should contain the following information:

1. a general description of the project and its purpose;
2. the lead public body and any other parties who are participating;

3. a description of the type of personal information that will be linked;
4. the anticipated submission date of the PIA to the Commissioner for review and comment; and
5. the contact information of the person responsible for completing the PIA.

Privacy Impact Assessment Content

The provincial Access to Information and Protection of Privacy (ATIPP) Office has issued directions to public bodies on how to complete a PIA. If a PIA is respecting a common or integrated program or service, *ATIPPA, 2015* requires the Minister to submit the PIA to the OIPC during the development of the project. Although the ATIPP Office provides directions on how public bodies must complete PIAs, the OIPC may require additional information when it reviews a PIA.

For example, the OIPC will require:

1. a detailed description of the project, including:
   (i) the project name;
   (ii) the expected project implementation date; and
   (iii) the contact information of the person responsible for completing the PIA;
2. a copy of your letter to the Commissioner providing early notice of the initiative;
3. a proportionality analysis explaining how the benefits of the project outweigh the risks to privacy;
4. an information flow diagram and legal authority for each data flow;
5. privacy risk assessment and mitigation plans; and
6. monitoring and/or audit plans.

Key Questions

- Has the public body identified and appropriately assessed risks to individuals, not just the organization?

- Have all data fields been identified?
  - Are they specific (individual fields versus mailing address, for example)?
  - Is the authority under which each field may be collected identified?
  - Does the PIA explain how each data field contributes to and is essential to achieve the identified purpose?

- Once the risks were identified, if there are a number of moderate to high risks, did the public body conduct an analysis based on the four part test of *R. v. Oakes*?
  - Is the measure demonstrably necessary to meet a specific need?
  - Is it likely to be effective in meeting that need?
  - Is the loss of privacy proportional to the need?
  - Is there a less privacy-invasive way of achieving the same end?

- Did the public body include enough detail about the overall operating environment and affiliate programs to conduct a thorough analysis? For example:
    - if end users are able to access information remotely through their own devices, details of the Bring Your Own Device (BYOD) program should be included;
    - if the program is depending on the general information protection education program for training, details of this program should be included;
    - if the program is in compliance with the information security infrastructure of the Department, details of this environment should be included.

- Did the public body include samples of materials developed to mitigate risks, such as privacy notices and consent forms?

OIPC Review Process

Once the Commissioner receives a PIA, an OIPC Analyst will review it. The Analyst may raise questions or seek clarification of the PIA from the public body. Based on feedback from other jurisdictions, the OIPC estimates the review process could take anywhere from a period of weeks to several months, depending on the robustness and amount of detail included in the PIA submitted. The OIPC recognizes that many PIAs cannot be finalized until the project is almost ready for implementation; the earlier the OIPC representative is included in the process and made familiar with the project, the quicker the review process will be. For example, even if a PIA is not available for review, inviting the OIPC to attend a meeting regarding the PIA, providing background information on the project, and providing copies of supporting documents, such as privacy notices or training materials for staff, will better ensure that the review is conducted in a timely fashion.

Public bodies should note that the OIPC's review and comment of a PIA will not be complete until questions raised by the Analyst have been addressed. Further, completion of a PIA review is not approval of the project. Although the OIPC's comments on a PIA are not binding per se, should the PIA reveal a collection, use or disclosure of a program or project is not in compliance with the *ATIPPA, 2015* it is possible for the Commissioner to launch an "own motion" investigation under section 73(3), which states:

> *73.(3)Where the Commissioner believes that personal information has been collected, used or disclosed by a public body in contravention of this Act, the commissioner may on his or her own motion carry out an investigation.*

Resource

This document is based on similar guidance developed by the Office of the Information and Privacy Commissioner in the provinces of Ontario and British Columbia. The Office of the Privacy Commissioner of Canada has also released expectations on PIAs submitted to their Office, as well as various other PIA resources.