Overview of a

PRELIMINARY PRIVACY IMPACT ASSESSMENT

Under the *Access to Information and Protection of Privacy Act, 2015*

Newfoundland
Labrador

Table of Contents

What is a Preliminary Privacy Impact Assessment?

A Preliminary Privacy Impact Assessment (PPIA) is a tool used to evaluate and mitigate potential privacy risks in a public body's projects or programs. A PPIA will also identify if a more comprehensive review of privacy issues (i.e. a privacy impact assessment (PIA)) is required.

A PPIA reviews the information handling practices of a public body (e.g. collection, use, disclosure, security and safeguards of personal information). It provides:

- A general overview of the project;
- The purpose of collections of personal information;
- Legislative authority to collect, use, and disclose personal information;
- A description of security safeguards;
- Level of risk with the project;
- Recommendations on how personal information can be protected; and
- Accountability and reassurance to end users that their confidential information is a part of the process

The ATIPP Office has developed a PPIA template for public bodies to use, which is available at: www.atipp.gov.nl.ca.

Why is a PPIA necessary?

ATIPPA, 2015 requires a PPIA or a full PIA be completed during the development of a program or service by a department or branch of the executive government of the province. The results of the PPIA or the PIA must be submitted to the Minister responsible for the Department of Justice and Public Safety – ATIPP Office for review and comment.

When completing the PPIA, a public body will review how personal information will be collected, used, access and/or disclosed, which includes reviewing:

- The type of personal information being collected;
- How personal information will be collected (i.e. directly from the individual or another source);

- Whether personal information will be disclosed, and to who (e.g. another public body, third party business, etc.);
- The purpose for the collection, use, access or disclosure (e.g. to determine eligibility for a service, for product registration, etc.);
- The manner in which individuals provide consent; and
- Which security safeguards (e.g., log–in credentials, single sign–on, access controls) will be implemented to protect personal information.

Who should complete a PPIA?

A PPIA should be completed by the program manager (team lead with the department or public body). Depending on the program or service being reviewed, it may be appropriate for the manager to consult the Office of the Chief Information Officer (OCIO)/IT department, as well as the public body's ATIPP Coordinator.

While completing the PPIA, the program manager should also consult with the ATIPP Office.

Role of the ATIPP Office

As mentioned previously, *ATIPPA, 2015* requires a PPIA or a full PIA be completed during the development of a program or service by a department or branch of the executive government of the province. The results of the PPIA or the PIA must be submitted to the Minister responsible for the Department of Justice and Public Safety – ATIPP Office for review and comment.

The ATIPP Office is available to assist any department or public body in completing a PPIA or PIA including answering questions on how to complete the assessment templates.

Once a public body has completed a PPIA, they should submit it to the ATIPP Office for review.

The ATIPP Office will then review the PPIA or PIA to assess what privacy risks may be present and whether adequate safeguards are in place or if any privacy risk exists and have been appropriately mitigated. Following its review, the ATIPP Office will write to the department or public body and provide a Privacy Impact

Report that outlines the legislative authority for collecting, using or disclosing personal information, any privacy risks identified, any safeguards and any recommendations it believes are appropriate to mitigate privacy risks.

The PPIA Process

The ATIPP Office has designed a streamlined process to review PPIAs as quickly and thoroughly as possible. The main steps are:

1. Review the PPIA Guidelines
2. Department/public body will obtain a copy of the PPIA Template
3. Department/public body will complete the first draft of the PPIA and submit to the ATIPP Office by email
4. The ATIPP Office will reply with clarifying questions or request a meeting to review
5. The PPIA is updated by the department/public body, where applicable
6. Risk analysis is completed by the ATIPP Office
7. Recommendations and/or signoff is provided by the ATIPP Office
8. The ATIPP Office will follow up on the implementation of any recommendations it provides within a specified timeframe.

What information do I need to complete a PPIA?

Generally, all that is required to initiate the PPIA process is an understanding of what the project or service is trying to achieve, what personal information is needed and how the information will travel through the program or service.

Additional information may also be required in the review process:

- Project overviews and charters
- Information sharing agreements
- Service contracts
- Application forms
- Website screen shots
- Information data flow charts and tables
- Legal advice

Examples of programs or services that require a PPIA

- New programs or initiatives that do or do not involved personal information,
- Updates to outfacing websites
- Changes to applications forms
- Merging programs with other public bodies

Final Sign-Off

Before the PPIA is finalized, the program manager (or another person with responsibility for the project) must review the completed PPIA. Once they have reviewed, their name should be included in the Sign-Off section of the PPIA which will be considered their sign-off on the PPIA.