ATIPPA, 2015 Guidance

Privacy Impact Assessments: An Introduction to ATIPPA, 2015 Requirements

Purpose

This guidance provides introductory information about Privacy Impact Assessments (PIAs) and examines requirements under the **Access to Information and Protection of Privacy Act, 2015** (ATIPPA, 2015).

What is a PIA?

A PIA examines a project in the context of the privacy principles, best practices, codes of conduct, legislation, and relevant directives. A well written PIA identifies the impacts that a project will have on privacy and suggests mitigation activities to lessen the impacts and risks. In general, PIAs should be conducted early enough in the project to allow the findings to be considered in the decision-making process. Even once the project is implemented, the PIA should be revisited if any further changes are proposed, if the overall operating environment changes, or as set out in the review schedule established in your PIA document. PIAs should be conducted for existing projects as resources allow.

In general, PIAs should be written in an easily understandable format and language. It should not contain jargon or project specific acronyms. The purpose of the PIA process is to identify privacy risks and identify mitigation activities; it is not meant to be a marketing tool that only shows the benefits of the project.

> A PIA is a systemic 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, An evaluation of PIA guidance documents. International Data Privacy Law

ATIPPA, 2015 defines a PIA in section 2(w), stating:

> "privacy impact assessment" means 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.

Part III of the Act addresses the protection of personal information and establishes requirements for collection, use, disclosure, as well as the ability for individuals to file a privacy complaint.

In general, it is best practice to conduct a preliminary PIA (PPIA) prior to starting a full PIA; the information gathered and insights gleaned from a PPIA may help determine the need for a full PIA report. In some circumstances, however, it will be clear from the outset that a full PIA is required.

Requirements for PIAs

ATIPPA, 2015 requires 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. 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 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.
>
> (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 or PIAs under ATIPPA, 2015, it is good practice to do so. In addition, while it is not required that OIPC review all PIAs, our Office welcomes the opportunity to review and provide comments on any PIA that is conducted by a public body.

Further, section 95 of 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 our Office has the authority to conduct investigations to ensure compliance with ATIPPA, 2015 and to monitor and audit practices and procedures employed in carrying out responsibilities and duties under 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?

While ATIPPA, 2015 does not define a common or integrated program or service, OIPC has adopted the following definition:

> A common or integrated program or service provides one or more services through:
>
> - a public body and one or more other public bodies working collaboratively; or
> - one public body working on behalf of one or more other public bodies.

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 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 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.

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. The length of the review period depends on the complexity and length of the PIA, as well as competing priorities. 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.

OIPC recognizes that many PIAs cannot be finalized until the project is almost ready for implementation; but 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 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 OIPC's review and comments on a PIA will not be complete until questions raised during the review have been addressed. Further, completion of a PIA review should not be construed as OIPC approval of the project.

Conclusion

PIAs are an important safeguard and are sometimes explicitly required under ATIPPA, 2015; even when not required, they are generally considered a best practice. Public bodies have a number of obligations under ATIPPA, 2015, and often a PIA is the best tool to allow a public body to demonstrate that it has made a reasonable effort to identify and comply with its statutory obligations. OIPC has developed a number of PIA resources to assist public bodies in ensuring compliance with ATIPPA, 2015 and privacy best practices; these are available online at Privacy Impact Assessments – Office of the Information and Privacy Commissioner.

Office of the Information and Privacy Commissioner
PO Box 13004, Station A
St. John's, NL A1B 3V8
Phone: (709) 729-6309
Toll Free: 1-877-729-6309
commissioner@oipc.nl.ca