Yukon Information & Privacy Commissioner

Guidance for Public Bodies:

PIA Reviews by the OIPC

January 29, 2015

Introduction

The only way for a **public body**[1] to effectively assess and manage privacy risks for any **project**[2] involving **personal information**[3] is to conduct a privacy impact assessment (PIA). Completing a PIA enables a public body to identify any risks associated with the collection, use or disclosure of personal information and ensure the information is properly managed in compliance with the *Access to Information and Protection of Privacy Act* (ATIPP Act).

The value of having the Office of the Information and Privacy Commissioner (OIPC) review a PIA is as follows:

- A public body is able to draw on the experience of the OIPC in interpreting and applying the ATIPP Act.
- It enables the public body to receive feedback from the OIPC about whether the project poses risks to the privacy of personal information.
- It demonstrates the public body's accountability for ensuring the risks to privacy associated with projects involving personal information are being appropriately managed.

Information that must be included in a PIA

In order for the OIPC to effectively evaluate whether a project undertaken by a public body poses risks to the privacy of personal information, any PIA submitted for review by the OIPC must contain, at minimum, the following information:

1. A description of the project.
2. The public body/bodies or other bodies involved in the project.
3. A diagram showing the flow of personal information and all collection, use and disclosure points within or between the public body/bodies or other body.

[1] A "public body" is the body under the ATIPP Act that is required to comply with the ATIPP Act for records in its custody and control.

[2] "Project" includes any new collection, use or disclosure of personal information or the modification of existing systems, programs or activities that involve personal information.

[3] "Personal information" is as defined in the ATIPP Act.

4. Identification of the public body/bodies or other body that has or have custody or control of the personal information and the public body/bodies or other body that is accountable for protection of the personal information.

5. An explanation as to why collection, use or disclosure of personal information is required for the project.

6. Clearly stated purposes for the collection, use and disclosure of personal information.

7. For the purposes identified, the specific authority to collect, use or disclose the personal information. As part of identifying the authority, the following information must be included.

    a. Identification of the relevant provision under section 29 for collection, section 35 for use, and section 36 for disclosure relied upon by the public body for authority. If an Act or provision is paramount to the ATIPP Act, the name of the Act and the provision relied on as authority.

    b. How the provision identified provides authority including why it is ***necessary*** to collect, use or disclose ***this*** personal information. As part of determining what is necessary, there must be information provided that identifies there was consideration of the sensitivity and amount of personal information and whether less sensitive or a less amount of personal information would suffice.

8. For personal information that will be collected indirectly, the provision relied upon and how this provision provides authority (subsection 30 (1)).

9. Whether there is a requirement to give notice about the collection, what the notice will contain and how notice will be given (subsection 30 (2)). If there is no requirement to give notice, the provision relied upon and why this provision applies (subsection 30 (3)).

10. If consent is relied on as authority to indirectly collect, use or disclose the personal information, the process that will be used, the content, and how a withdrawal or limited consent will be managed. If consent is not relied on for this authority and is a reasonable option, why this decision was made.

11. If the personal information will be used to make a decision that affects the individual, the effort that will be made to ensure the accuracy of the personal information (section 31).

12. The process that will be used to correct or annotate the personal information (section 32).

13. The **privacy management program components**[4] in place and a description of how these components will protect the privacy of the personal information (section 33). Documented evidence of the privacy management program components along with all the program controls must be attached. It must also be demonstrated in the PIA that the sensitivity of the information was evaluated in determining what is required to properly protect the personal information from a privacy breach. Where there is a significant risk to the protection of personal information a security threat risk assessment should accompany a PIA.

14. If personal information will be used to make a decision that directly affects an individual, the process to ensure the personal information will be retained for one year after it is used to make the decision (section 34).

15. If the personal information will be disclosed for research:

    a. why the research cannot be accomplished without using personal information,

    b. if there is any data linking involved in the research:

        i. why the data linking will not be harmful to the individuals the information is about, and

        ii. why the benefits to be derived from the data linkage are in the public interest, and

    c. a copy of the agreement entered into between the public body and researcher must be attached (section 38).

16. How access to personal information will be facilitated (subsection 5 (1) and section 36).

17. An evaluation of the risks to the privacy of the individuals whose personal information is involved in the project and an analysis of these risks measured against the benefits to be achieved by the project. If the evaluation demonstrates the risks to privacy outweigh the benefits of the project, an explanation as to why the public body feels the project should proceed.

18. Any risks associated with the ability to meet the requirements of the ATIPP Act should be documented in a chart along with a strategy to mitigate each risk. The strategy must include timelines for completion that are reasonable in light of the risk.

[4] The "privacy management program components" are those identified in Guidance for Public Bodies on Accountable Privacy Management prepared by the OIPC.

Additional Information May Be Required

As the OIPC cannot anticipate the complexities associated with every project involving personal information, the OIPC may request information not included in this guidance where necessary to properly evaluate the risks to privacy associated with a project.

Process following a PIA review

Following a PIA review, the OIPC may issue comments and recommendations to mitigate risks of non-compliance with the ATIPP Act or to privacy more generally. If the recommendations are accepted by the public body/bodies, the OIPC may accept the PIA. The OIPC will only accept a PIA if satisfied the risks identified in the PIA have been mitigated or will be mitigated within a reasonable timeframe. If the recommendations are not accepted by the public body/bodies and the OIPC is not satisfied the risks are or will be mitigated, the OIPC will not accept the PIA.

The submission, acceptance and non-acceptance of PIAs are reported in the IPC's Annual Report.

Questions about the content of this document should be forwarded to:

Office the Information and Privacy Commissioner
Suite 201, 211 Hawkins Street
Whitehorse, Yukon Y1A 1X3
Telephone: 867-667-8468 Toll Fee: 800-661-0408 ext. 8468
Email: info@ombudsman.yk.ca

This document was prepared to assist the public and public bodies subject to the *Access to Information and Protection of Privacy Act* (ATIPP Act) understand what the Office of the Information and Privacy Commissioner requires to review PIAs and what the process for review will entail. The document is for administrative purposes only and is not intended, nor is it a substitute for legal advice. For the exact wording and interpretation of the ATIPP Act, please read the Act in its entirety. This document is not binding on the Information and Privacy Commissioner.

As this document is used for administrative purposes it is subject to change without notice. Please refer to the Office of the Information and Privacy Commissioner's website at www.ombudsman.yk.ca for the current version.