Fact Sheet: Privacy Impact Assessments

The *Protection of Privacy Act* (POPA) establishes that public bodies are required to prepare privacy impact assessments (PIA) under prescribed circumstances and in some cases, to submit them to the OIPC.

Overview

Conducting PIAs is an exercise to assist public bodies in identifying and addressing privacy risks associated with the implementation of any new or changing administrative practice, program, project or service.

The process helps a public body by:

- Strengthening privacy and transparency by clearly identifying how personal information is collected, used, disclosed and retained.
- Managing risks related to personal information and data derived from personal information in their custody or control.
- Fulfilling compliance obligations under the POPA and regulations.

The PIA documents these due-diligence activities, helps in making informed decisions related to any administrative practice, program, project or service by understanding how privacy requirements are addressed and the safeguards implemented. PIAs can also highlight high-risk issues, prompting consideration of alternative technologies, products, or service designs, potentially saving time, cost, and preventing breaches.

A PIA's depth depends on the complexity of the administrative practice, program, project or service. PIAs help understand information flows and risks, even for projects that rely on non-personal data allowing for additional safeguards to prevent re-identification or misuse. As a best practice PIAs should be reviewed over time to ensure they are current, and amendments completed should there be significant changes.

A PIA must provide a level of detail that takes into consideration the complexity of the practice, program, project or service the privacy impact assessment relates to. This means each PIA can be tailored based on the size and complexity of the project and in general a PIA:

- Identifies and reviews risks associated with the public body's collection, use and disclosure of personal information,
- Develops mitigation strategies and safeguards respecting those risks,
- Address how the public body will comply with its duties under this Act, and
- Complies with requirements detailed in the Protection of Privacy (Ministerial) Regulation section 7(2).

When to complete a PIA

A public body can prepare a PIA for any circumstance when personal information is collected, used or disclosed. Section 7(1) and 7(5) of the Protection of Privacy (Ministerial) Regulation outlines when a PIA is required.

A PIA is only required for a new, or a substantial change to an existing, administrative practice, program, project or service if one or more of the following apply:

- if the loss of, unauthorized access to or unauthorized disclosure of the personal information could result in significant harm,
- a practice, program, project or service will collect, use or disclose personal information considered to be of high sensitivity,
- a practice, program, project or service will involve the personal information of a significant percentage of the population the public body serves,
- a practice, program, project or service will involve data matching between 2 or more public bodies,
- a practice, program, project or service is part of a common or integrated program or service, or
- a practice, program, project or service involves the development or use of innovative technology.

PIA Contents

A PIA completed by a public body, as required under section 7 of the Protection of Privacy (Ministerial) Regulation, must:

- Include a summary of the purpose of the collection, use or disclosure of personal information for the new, or substantial change to an existing, administrative practice, program, project or service,
- Identify the legal authorities for the collection, use or disclosure of the personal information,
- Identity of any privacy risks and mitigation strategies respecting the personal information,

- Identify or describe any administrative, physical and technical safeguards in place to protect the personal information, including how the personal information will be securely transmitted, matched or linked by the public body, if applicable,
- A description of the accuracy, correction and retention procedures that will be implemented to ensure the personal information is accurate and complete, and
- The establishment of a clear governance structure respecting the responsibilities and accountability of each public body if 2 or more public bodies are engaging in a common or integrated program or service or if a public body is collecting personal information from another public body under section 17(3) of the POPA for the purpose of carrying out data matching.
- Where there is a common or integrated program or service or data matching between 2 or more public bodies, the public bodies involved in the common or integrated program or service may prepare a joint privacy impact assessment; however, each public body must prepare an addendum to address any unique collection, use or disclosure circumstances that apply to that public body.

Note there is nothing in the Act or regulations preventing public bodies from jointly preparing a PIA. There are times when public bodies may be using the same systems or technology (for example Microsoft 365, or school boards that jointly use a system) and they may wish to jointly complete a PIA with addendums that respond to public body specific implementation of the program or service could be considered.

Amendment to PIAs

If there is a substantial change to an existing administrative practice, program, project or service for which a PIA has already been completed, the public body may amend the PIA to reflect the change. An amendment updates and replaces relevant portions of the original PIA to ensure it accurately reflects the current state of implementation of the practice, program, project or service.

Addendum to PIAs

Where a common or integrated program or service or data matching activity, involves two or more public bodies and a joint PIA has been prepared, each public body must prepare a PIA addendum to address any collection, use or disclosure circumstances unique to that public body. An addendum supplements the original PIA by adding new information and does not alter the content of the original document. As a best practice, any agreements documenting the common and integrated program or data matching should be included in the PIA addendum.

Submitting to the Information and Privacy Commissioner

Public bodies are required to prepare and submit a PIA to the Information and Privacy Commissioner for the following types of projects:

- a practice, program, project or service will collect, use or disclose personal information considered to be of high sensitivity;
- a practice, program, project or service will involve the personal information of a significant percentage of the population the public body serves;
- a practice, program, project or service will involve data matching between 2 or more public bodies;
- a practice, program, project or service is part of a common or integrated program or service;
- a practice, program, project or service involves the development or use of innovative technology.

Refer to the Information and Privacy Commissioner's website for mandatory requirements for submitting a PIA to that office under POPA as well as other useful PIA resources. NOTE: The OIPC requires the use of their POPA PIA template.

The Information and Privacy Commissioner may also request a copy of a PIA under POPA section 27(1)(j). A public body has thirty business days to provide a copy of the requested PIA. Best practice for a public body should include a listing of completed PIAs for reference.

Related Resources

***Protection of Privacy Act* Guide**

Fact Sheet: Privacy Management Programs

Fact Sheet: Common or Integrated Program or Service

Fact Sheet: Data Matching and Data Derived from Personal Information

Fact Sheet: AI and Automated Systems