# Privacy Impact Assessments – Overview

Privacy Impact Assessments (PIAs) help to identify, mitigate and monitor privacy risks in any new, or substantially modified program or activity. The Treasury Board Secretariat's Directive on Privacy Practices requires that federal institutions conduct PIAs:

- When personal information may be used as part of a decision-making process that directly affects an individual;
- When there are major changes to existing programs or activities where personal information may be used for an administrative purpose;
- When there are major changes to existing programs or activities as a result of contracting out or transferring programs or activities to another level of government or to the private sector; and
- When new or substantially modified programs or activities will have an impact on overall privacy, even where no decisions are made about individuals.

## 10 key steps in the PIA process

1. **Determine** the legal authority for your program or activity. Institutions can only collect personal information that is directly related to an operating program or activity of the institution.
2. **Contact** your ATIP office to help determine if a PIA, or other type of privacy assessment, is appropriate. Engage key stakeholders such as legal and IT services.
3. **Identify** the scope of your PIA.
4. **Consult** with the Office of the Privacy Commissioner of Canada (OPC) early in the process.
5. **Describe and document** what personal information is collected, how it is collected, used, disclosed and stored as well as measures to protect against inappropriate access or disclosure.
6. For intrusive or privacy-invasive initiatives or technologies, think through:
   - **Necessity** – What is the need for personal information?
   - **Effectiveness** – Will the personal information you collected meet that need?
   - **Proportionality** – Is the need proportional to the potential loss of privacy?
   - **Intrusiveness** – Is there a less privacy-invasive option?
7. **Draft** an action plan to implement mitigation measures, outlining roles, responsibilities and timelines.
8. **Submit** your PIA to the OPC and to the Treasury Board Secretariat (TBS).
9. **Consider** the recommendations provided to your institution.
10. **Monitor** privacy issues on an ongoing basis. PIAs should be updated over time as information flows evolve.

## Fundamental privacy principles to consider

**Accountability**
Designate an individual to be responsible for your personal information handling practices.

**Limiting collection**
Only collect personal information that is directly necessary to meet a program's objective.

**Direct collection and purpose identification**
Collect personal information directly from the individual and inform them of the purpose.

**Retention**
Only keep personal information as long as necessary. (*Privacy Act* regulations cite at least two years following the last administrative use.)

**Accuracy**
Institutions must take reasonable steps to ensure the accuracy of personal information.

**Disposal**
Institutions must securely dispose personal information in accordance with its records disposition requirements.

**Limiting use**
Institutions should only use personal information for the purpose for which it was collected, or for a consistent use.

**Limiting disclosure**
The disclosure of personal information should be limited, and in line with the original purpose of collection or a consistent use, or otherwise with the consent of the individual.

**Safeguards**
Institutions must take steps to appropriately protect personal information from inappropriate access, use or disclosure.

**Openness**
Be open and clear about how personal information will be handled, for example, in privacy notices. Publish PIA summaries.

**Access**
Individuals have a right to request access to their personal information, and correct it, when necessary. Develop and document a process for responding to requests.

For more detailed guidance on preparing PIAs, please consult the OPC's Guide to the Privacy Impact Assessment Process and the TBS Directive on Privacy Practices.