# Expectations: OPC's Guide to the Privacy Impact Assessment Process

Revised: March 2020

## Table of Contents

Section 1 – Purpose
Section 2 – Context
Section 3 – Role of the OPC
The Government Advisory Directive
Consultation and Preparation
How to Read the OPC's Government Advisory Directives
Section 4 – Privacy impact assessments
What is a PIA and what is its purpose?
When is a PIA required?
Documenting the decision
Other assessments and procedures
What should a PIA include?
Planning phase
Planning phase
Risk Analysis Phase
Preliminary risk assessment
Risk factors
Low complexity, low risk programs
Questions for high risk programs: necessity, effectiveness, proportionality and minimal impairment
Assessment of privacy impacts
Risk analysis for privacy principles
Accountability
Limiting collection
Direct collection and consent; identification
Retention
Accuracy
Disclosure
Limiting use
Limiting disclosure
Safeguards
Openness
Individual access
Risk mitigation phase
Action plan
Drafting phase
PIA report-level practices
Approval phase
Reporting phase
Review phase
Acknowledgements
Disclaimer

## Related content

The Tips and Templates for Privacy Impact Assessments

## Section 1 – Purpose

This document provides guidance to federal public sector institutions on how to comply with the Privacy Act and effectively manage privacy risks as part of the privacy impact assessment (PIA) process. It presents key concepts and tips on how an institution may assess its programs and activities, including how to document the decision-making process.

The Office of the Privacy Commissioner of Canada (OPC) recommends that institutions use this document as a guide when undertaking PIAs and consult with respect to the PIAs as needed.

## Section 2 – Context

The Privacy Act requires institutions to assess to collect, store, analyze, and share large amounts of personal information in order to fulfill their mandates and provide programs or services to Canadians and other residents. Civil litigations has created new opportunities for organizations to more effectively accomplish their mandates, but it has also created new risks to the privacy of individuals. The Privacy Act, as a rights based policy, was drafted in the Canadian Charter of Rights and Freedoms's quasi-"step-child" status. Not surprisingly, the Privacy Act does not contain provisions that are "Charter proof".

Government institutions hold much more personal information today than when the Privacy Act became law in 1983. Institutions need to be more accountable and justify their collection, use and disclosure of personal information.

Individual privacy is not a right as can be easily quantified using revenues, efficiency or commercial gain. Individual privacy is a constitutionally protected right. It is only when we concerned about that privacy which engages that having personal privacy protection is not just a legal requirement, it is essential to maintaining our democratic institutions.

Institutions need to be able to demonstrate that they have the tools to manage personal information. Institutions need to be able to demonstrate that they have the tools to collect, store, analyze, share and destroy personal information lawfully and in a manner that respects individuals' privacy. This means that institutions need to be able to demonstrate that they have the tools to manage privacy risks. The PIA is one such tool.

In a society's environment, assessing potential privacy risks is more important than ever.

While PIAs are currently a requirement of a TBS policy, the authors have recommended to Parliament that the Privacy Act be amended to require institutions to:

- conduct PIAs for new or significantly amended programs involving personal information;
- submit their PIA reports to the OPC before implementing a program or activity.

Parliament has recognized that PIAs are a tool that can be used to ensure that institutions are more and that privacy impacts are taken into account when developing programs and activities. In other parts of the world such as Europe, PIAs are becoming the legal standard.

## Section 3 – Role of the OPC

### The Government Advisory Directive

The OPC's Government Advisory Directive provides guidance to federal public sector institutions on how to comply with the Privacy Impact Assessment Directive. We provide additional guidance on:

- consultations
- reviewing PIA reports, information sharing agreements, and notifications under s. 8(2)(e) and s. 9(4) of the Privacy Act
- conducting ministerial engagements

### Consultation service and report review

The OPC is pleased to offer consultation on PIAs. However, institutions don't need PIAs of a stage with us on privacy issues. The OPC can provide federal institutions with more informal, practice advice and guidance on how to address privacy issues and risks.

Many programs and activities raised complex legal issues and institutions may want to consult with us prior to the OPC at the same time they provide them to TBS. However, we encourage you to consult as long as you have sufficient time to allow us to provide our advice. We understand that institutions have tight deadlines and sufficient advice is sometimes required for development and implementation of large or complex programs and activities.

The OPC has received its contract the OPC at one stage for assistance or identifying compliance issues as well as risks to privacy and potential mitigation strategies.

Once the PIA report is completed, we review the **final** version, and provide written recommendations where we have privacy issues or concerns. We may also review, depending on our office's workload, a PIA report that is in development or in progress.

### Section 4 – Privacy impact assessments

### What is a PIA and what is its purpose?

A PIA is a tool management process that helps institutions ensure they meet legislative requirements and identify the impacts their programs and activities will have on individuals' privacy.

A PIA should include the following elements:

- legal requirements and set out the Privacy Act
- the institution's program or activity
- the personal information involved in the institution's policies and directives.

Adhering to the requirements alone will reduce the risk of complaints or unauthorized collection, use, disclosure, retention or disposal of personal information.

Many programs and activities raised complex legal issues or privacy requirements, they should also be considered in the context of the institution's mandate and the institution's overall privacy management. For example, you should seek to reduce the risk that an individual may suffer harm, such as identity theft, reputational harm, or humiliation, as a result of a breach of his or her personal information. If they are individuals such harm or humiliation can should lead to identity and credit fraud. There is other more low-risk way of designing a project. A PIA can help identify the least privacy intrusive way of designing a program or activity.

PIAs can and are being updated, allowing institutions to identify and mitigate risks to privacy as complete as possible. They are a key tool for decision-makers, enabling them to deal with issues proactively and to make informed decisions about the privacy implications of their programs.

An effective PIA may build trust with Canadians by demonstrating due diligence and compliance with legal and policy requirements as well as privacy best practices.

A PIA should be a living document. The PIA can also assess future risks to privacy such as part of the collection of personal information for a program.

**Tip:** Institutions should ensure compliance with the Privacy Act. Even when a program is legally compliant, you should identify and manage the risk that it may negatively impact the privacy of individuals. Where possible eliminate impacts altogether.

### When is a PIA required?

PIAs are required under the TBS Directive on Privacy Impact Assessment and have been a policy requirement since 2002.

A PIA is generally required if your program or activity may have an impact on the personal information of individuals. Institutions should also consider the following factors when deciding to conduct a PIA:

- where personal information may be used as part of a decision-making process that directly affects the individual
- where there are changes to existing programs or activities where personal information may be affected, or where personal information may be used for administrative purposes affecting individuals
- where there are changes to Privacy Impact Assessments; institutions are required to update their transferring programs or activities to another level of government or to the private sector

The Privacy Act defines personal information as "information about an identifiable individual that is recorded in any form". Example of personal information include: name, address, employment history, fingerprints, medical diagnosis and treatment records.

Examples of administrative uses of personal information include using personal information to:

- to decide whether an individual can enter the country
- to determine an individual's eligibility to receive a social service
- to investigate an individual for possible wrongdoing

You may decide to conduct a PIA for your institution even in substantially changed programs or activities where the institution's mandate does not change. The OPC recommends that institutions use PIAs to encourage institutions to undertake a PIA if that program or activity will have an impact on privacy and individuals' rights and freedoms. Institutions should consider the risk that a PIA may be required if they do not do a PIA in such circumstances. Thoroughly assessing risks to privacy through a PIA can help decision-makers legally compliant and privacy-friendly programs.

Institutions should consider the risk that a PIA may be required in the document is helps you determine your program or activity's privacy impact. Institutions may use a sample of the risk-based approach to assessment you may choose to conduct a PIA even when there is no administrative use of personal information. Institutions should consider such an approach when conducting a PIA, or not doing a PIA.

**Tip:** It is important to assess the privacy impacts of new as well as old initiatives. Conduct PIAs for programs and activities that are being redesigned, implemented, or, moreover, after. Begin with programs and activities likely to pose the greatest risk.

**Use this flowchart to help you determine if you need to do a PIA**

▶ Text version of Figure 1

### Documenting the decision

If you decide not to conduct a PIA, document your decision and the rationale. As a best practice, you should identify and address the privacy impacts of your programs and activities even when you do not do a formal PIA.

### Other assessments and procedures

Consider whether you should complete other formal assessments or procedures along with or instead of a PIA.

Whenever PIAs intersect with or cover other assessments or audits by privacy-powerful programs and activities, other assessments have different areas of focus. For example:

- **Threat and risk assessments** identify potential threats to information and controls to establish the extent to which they are implemented correctly and achieving the desired outcome and identify residual risks that should be accepted
- **Security assessments** identify and prioritize a department's critical services and assets to allow the selection of suitable measures to manage risks to the availability of those services and assets
- **Algorithmic impact assessments** identify and mitigate risks associated with deploying an automated decision-making system.

Consult TBS policy suites to determine whether other assessments or procedures may be required.

**Tip:** If the scope of questions posed in the Directive on Privacy Impact Assessment is in the guide to conducting a PIA, you may want to undertake a PIA. In the assessment you should be doing! You can always transport out an PIA to conduct a PIA even when there is no administrative use of personal information.

**Tip:** It is important to assess the privacy impacts of new as well as old initiatives. Conduct PIAs for programs and activities that are being redesigned, implemented, or, moreover after. Begin with programs and activities likely to pose the greatest risk.

### What should a PIA include?

The TBS Directive on Privacy Impact Assessment sets out content that must be included in PIA reports. You should consult the Directive to ensure that your PIA complies.

In general, your PIA report should include:

- a description of the planned program or activity and its objectives
- a description of the personal information involved in the program or activity
- the necessary authorities for collecting, using, and disclosing personal information
- the necessary consultations
- the necessary consultations
- the necessary consultations

Institutions should also consider the following elements in their documentation:

- Program staff: that is, the person or people responsible for developing and delivering the program or activity
- Privacy staff: including your Access to Information and Privacy (ATIP) group and your Chief Privacy Officer or equivalent
- Internal legal counsel
- Information Management (IM), information technology (IT) and security as required
- Other staff as required
- Program managers: if involved in developing or delivering the program or activity
- The senior official or executive responsible within the institution for new or substantially changed programs or activities involving personal information, and
- Heads of government institutions are required to delegate to sections 10 to 13 of the Privacy Act, and to report on such delegations in their annual reports to Parliament.

You may not need to engage all of the partners listed above for each PIA; however, at a minimum, involve relevant program and privacy staff in the PIA process.

**Tip:** It is consultant is considering your PIA, ensure you have capacity within your institution to implement recommendations and engage with the OPC prior that contract is over.

Multi-institutional PIAs:

- Where two or more institutions intend to establish a common initiative or a share information, it may be preferable to undertake a multi-institutional PIA (MIPIA).
- These institutions PIAs may be a joint consultation of a program or activity. The OPC may be consulted on a MIPIA.
- When different institutions, as separate PIAs or small components of a shared program or a new program, the OPC may be consulted on the PIA.
- Multi-institutional PIAs may be redacted the chances of gaps or inconsistencies.
- Multi-institutional PIA reports should clearly set out which party is responsible for addressing risks. Program managers or lead institutions with overall responsibility for the PIA.

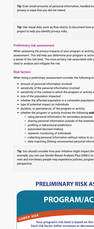
**Tip:** Ideally institutions will conduct one multi-institutional PIA where they are involved in delivering a program or activity. Institutions may also want to consider conducting a PIA for a program or activity they intend to implement, even if they are not the lead. Institutions should clarify that you clearly prepared.

Consult the OPC:

- The OPC's Gov Directive provides advice to institutions related to specific programs and activities involving personal information. Institutions should review the Gov Directive.
- Consult the Informations, see Section 3 – Role of the OPC.
- Institutions should consult the OPC on PIAs, MIPIAs, or other documents, such as information sharing agreements or activities that could impact privacy – whether or not a PIA is planned.

At the end of the planning phase you should identified the scope of the PIA, the necessary resources, the governance structure, the risks and risks and the timeframe for the process.

**The PIA Process**




▶ Text version of Figure 2

### Risk analysis phase

All of your institutions's activities involve some kind of risk. Institutions manage risk by identifying it, analyzing it and evaluating whether the risk needs to be mitigated.

Risk is the chance that something will happen that will impact on your institution's objectives and priorities. Risk is also the chance that something will happen that will affect individuals.

Risk can also be measured in terms of its impact on them. If it occurs.

A PIA's focus is not on the group – that is, risk posed to the individual's privacy and rights under the Charter. Institutions should consider the risk to individuals' privacy and rights when they consider the risk to their institution and implement the PIA process. It is important to be clear on the institution's requisites. Financial losses or emotional well-being or pain.

Institutions should consider the risk to their program or activity when the event occurs negatively to see (the more efficient order impact).

**SEVERITY** + **LIKELIHOOD** = **RISK LEVEL**

When you have determined that your program or activity may negatively impact an individual's privacy, there is a risk that your institution is not complying with its obligations under the Privacy Act. Address legal non-compliance immediately.

**Tip:** Even small amounts of personal information, handled inappropriately, can impact someone's privacy in ways that you did not intend.

**Tip:** Use visual aids, such as charts, to document how you will use information as part of a program to identify privacy risks.

### Preliminary risk assessment

When assessing the privacy impact of your program or activity, it is a good idea to do a preliminary risk assessment. This will help you determine your program or activity's potential privacy impacts and give you a sense of the risks. It will also help you determine whether your program or activity has low-risk privacy impacts and is eligible for a streamlined PIA.

### Risk factors

When doing a preliminary assessment consider the following risk factors:

- amount of personal information involved
- sensitivity of the personal information involved
- sensitivity of the context in which the personal information is used
- size of the population impacted
- the relationship between the institution and the vulnerable population
- type of personal impact on individuals
- duration, or permanence, of the program or activity
- **Other factors to consider when conducting a preliminary risk factors**
- using personal information for a new purpose
- disclosing personal information outside a jurisdiction
- profiling or behavioural predictions
- automated decision-making
- systemic monitoring of individuals
- collecting personal information without notice to or consent of the individual
- using Data Linking (combining personal information from different sources)

**Tip:** You should consider how your initiative might impact the privacy rights of different groups. For example, a program or activity may have a low risk for the majority of the population but have a high risk and serious people who experience policies, programs and initiatives from a privacy perspective.

## PRELIMINARY RISK ASSESSMENT

**PROGRAM/ACTIVITY**

| LOW RISK | MEDIUM RISK | HIGH RISK |
|---|---|---|
| **Your program's risk level is based on the total of all factors.** | | |
| Does not involve personal information | Involves the use of non-personal information | Involves the use of personal information |
| Does not involve sensitive personal information | Involves sensitive personal information such as financial or medical information, or social insurance numbers | Involves sensitive personal information |
| Contains no sensitive | Contains a sensitive | Contains a sensitive |
| Involves the personal information of a few individuals | Involves the personal information of many individuals | Involves the personal information of many individuals |
| Does not involve personal information from vulnerable populations | Involves personal information of one vulnerable population | Involves personal information from multiple vulnerable populations |
| Has a minimal impact on individuals (e.g. lower stakes) | Has a major impact on individuals (e.g. higher stakes) | |
| Is one time or short term | Is long term | Involves one or more of the additional factors can additional risk factors above |
| Does not involve the additional risk factors can additional risk factors above | Involves one or more of the additional risk factors above | |

▶ Text version of Figure 3

### Low complexity, low-risk programs

Institutions can use the PIA process to design programs or activities that are suitable. The length and complexity of your PIA report should be proportionate to the risks, complexity and size of your program. If, based on your preliminary risk assessment, you determine that your program or activity is low risk, you may want to consider a streamlined PIA process and prepare a shorter report.

Even if PIA is a low-complexity, low-risk initiative should address all key components in sufficient detail, but you may find that:

- fewer parties need to be involved in the process
- fewer stakeholders need to be consulted
- these are limited information flows to map
- there are few or no privacy risks to address
- there are fewer privacy impacts and therefore fewer recommendations to discuss
- the PIA is shorter.

Not complying with our or office policy in the process, you can provide guidance on how to conduct an PIA.

### Questions for high risk programs: necessity, effectiveness, proportionality and minimal impairment

Institutions that undertake privacy impact assessment programs have established the importance of ensuring that the intended outcome and objectives of a program or activity and initiatives are carefully evaluated at the outset. This should assess high-risk or privacy-invasive programs or activities in the context of their potential impacts on individuals. This is a key part of the process of identifying and mitigating privacy risks. Institutions should find the language of whether the program or activity is proportionate to its purported benefits. Are these expectations of privacy protections are an effectively-sized voice program or activity is privacy-developed.

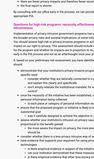
Institutions can use proportionality and minimal impairment to assess the privacy impacts of their program or activity.

- demonstrate that your institution's privacy-invasive programs or activities are necessary to meet a specific need
- consider whether they are rationally connected to a public good that is important to society and impair this should and specifically
- ensure that the program or activity is proportionate to its purpose, "low enforcement" or "border security"
- ensure that the collection of the relative harm that institutions may cause to individuals' privacy or personal information being collected
- ensure that the personal information being collected is necessary to achieve the goal
- ensure that proposed program or initiative is likely to be effective in meeting the purpose and substantial goal
- ensure that the program is achieves the objectives in question?
- assess whether your institution's innovative program or activity is proportionate to its purpose, and that it is not arbitrary, unfair or based on irrational considerations
- the harm severe the respect or privacy the more pressing and substantial the public good should be
- consider whether there is a less privacy-invasive way of achieving the same end
- have evidence that supports your argument for using privacy-invasive or invasive activities or programs
- is there empirical evidence to support the initiative?
- test your institution demonstrates that these measures are effective in meeting stated goals?
- consider whether the privacy-invasive measure is minimally impairing of the rights of individuals?

If your institution cannot explain how your initiatives proposed collection, use or disclosure of personal information is necessary to meet a specific need or how it is likely to be effective in meeting its intended purpose, it may be time to reconsider whether the initiative's objectives are worthwhile or whether it should be pursued in the manner proposed. Institutions should be able to show that their initiatives are necessary, effective, proportional and minimally invasive before proceeding with implementation.

**Tip:** While the questions discussed above are necessary for assessing the privacy impacts, they are also useful questions to ask when beginning any project and can help to ensure that key privacy considerations are taken into account at the outset.

**ROADMAP FOR HIGH RISK PROGRAMS**




## Assessment of privacy impacts

### Risk analysis for privacy principles

### Accountability

### Limiting collection

### Direct collection and consent; identification

### Retention

### Accuracy

### Disclosure

### Limiting use

### Limiting disclosure

### Safeguards

### Openness

### Individual access

### Risk mitigation phase

### Action plan

### Drafting phase

### PIA report-level practices

### Approval phase

### Reporting phase

### Review phase

### Acknowledgements

### Disclaimer

1. Consider the impacts of your proposed program or activity on individuals' privacy. Identify and mitigate risks arising from collection and use of personal information and other factors that could result in unfair or arbitrary decisions made by program or activity decision-makers.

2. Ask key questions to evaluate the necessity, effectiveness, proportionality and minimal intrusiveness of your initiative

3. Discuss your results prior to proceeding with privacy review or consultation with your privacy office and senior officials responsible for your program

4. Ensure high risk programs or activities are accompanied by effective, proportional and minimally intrusive measures to address their implementation.

▶ Text version of Figure 1

## Risk analysis by privacy principle

If you are developing a project that involves personal information, you must comply with the Privacy Act. Section 4 of the Privacy Act requires that personal information collected by a government institution must be relevant to the operations of Government of Canada. After ensuring your compliance with the Privacy Act, you should also consider how your initiative will impact the privacy rights of individuals.

As you analyze risks to the privacy of individuals and proposed program mitigating measures, we recommend that you assess your program against the principles below. These are based upon the Organization for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Fair Information Principles, which have shaped all largely undeclared privacy and data protection legislation in Canada, and the Canadian Standards Association Model Code for the Protection of Personal Information. These principles are not intended to impose any new obligations on your program, but they do impose requirements, that identify and negotiate impacts on privacy as well as mitigations. Depending on the nature and scope of your program or activity, some principles may be more relevant than others. The OECD privacy principles are not exhaustive. You may have other questions or measures to ensure that your program is **as or more intrusive that you meaningfully analyze the privacy impacts of your initiative.**

**Organization for Economic Co-operation and Development (OECD):** The OECD is a forum where governments work together to address the economic, social and governance challenges of the globalization. For several decades, the OECD has been playing an important role in promoting international instruments aimed at the protection of privacy and personal data. Its Guidelines governing, in 1980, the OECD introduced the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the first internationally agreed upon set of privacy principles. As an OECD member country, Canada participated in the development of these Guidelines and subsequently implemented the "Canadian version" of international Fair Information Principles in Canada.

See the OECD Privacy Guidelines (more information on the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).

### Accountability

**Relevant legal instrument:** Privacy Act s. 4

**Relevant policy instrument:** Policy on Privacy Protection and Directive on Privacy Practices

**What "accountability" means:** Put someone in charge of your institution's handling of personal information and develop privacy policies, procedures and training.

**Questions to consider:**

- Who is responsible for your institution's compliance with the Privacy Act and privacy best practices?
- What policies and procedures does your institution have in place to protect privacy?
- Do your policies and procedures do more than simply parroting the wording of the Privacy Act specific obligations?
- How do you ensure staff receive privacy training?
- Do your staff, from the top down, understand and are resistant to managing personal information?
- What is the process for reviewing, assessing and responding to privacy compliance and breaches?

**Risk example:**

- Your program may not know who to contact about privacy questions or concerns
- Staff may be confused about how to protect personal information
- Privacy breaches may not be identified and shared with the person accountable for compliance with the Privacy Act

**Mitigation example:**

- Make clearly the identified of individuals responsible for your institution's personal information handling practices here
- Develop your institution's informational handling guidelines or statements of fair information and for specific initiatives, as appropriate
- Ensure your institution's employees know to staff about the institution's policies and practices
- Monitor and institutionalize handling of personal information
- Develop a process for receiving, assessing and responding to privacy complaints and inquiries

### Limiting collection

**Relevant legal instrument:** Privacy Act s. 4

**Relevant policy instrument:** Directive on Privacy Practices and Directive on Social Insurance Number

**What "limiting collection" means:** Only collect personal information if it is directly affiliated to your initiative and its legal authorities.

**Questions to consider:**

- Why do you need to collect this piece or category of personal information?
- Is personal information "nice to have" or "need to have" for your initiative?
- Are there ways to organize that allow you to collect less information?

**Risk example:**

- An individual's personal information could be collected when it is not related to or necessary for a program or activity
- Personal information could be collected without a clear purpose

**Mitigation example:**

- Have a clear purpose for collection and collect only that personal information necessary for the identified purpose
- Use systems that will not identify individuals, when possible
- Design forms and systems so that only the information required is likely to be collected
- Review forms, systems and practices to ensure they are limiting collection
- Conduct a data minimization exercise to question the need for each piece of personal information collected or received
- Where even collection occurs, appropriately dispose of or return personal information as soon as possible

**Tip:** Case personal information that is publicly available should only be collected where it relates directly to or substantially supporting a program or activity.

### Direct collection and purpose identification

**Relevant legal instruments:** Privacy Act s. 5(1) and (3)

**Relevant policy instrument:** Directive on Privacy Practices

**What "direct collection" and "purpose identification" means:** When you collect commercial personal information, collect it directly from them whenever possible and tell them why you need it.

**Questions to consider:**

- Do you collect all of an individual's personal information for collection?
- If you are collecting an individual's personal information from other individuals or sources, why?
- Have you identified a purpose of the purpose for collection of the personal information?

**Risk example:**

- Individuals may be unaware of the collection, and subsequent use and disclosure of their personal information
- Information collected from other sources may be inaccurate, out of date or incomplete
- Individuals may be misled about the purpose for which their information is being collected
- Personal information could be collected without a clear purpose

**Mitigation Example:**

- Collect personal information from individuals whenever possible
- Notify individuals of the purpose for collecting and disclosing their personal information
- Whenever possible, notify individuals at or before the time of collection
- Ensure individuals understand the purpose for collecting their personal information
- Notify individuals of the purpose for collecting their personal information

### Retention

**Relevant legal instruments:** Privacy Act s. 4 and 6(1); Privacy Regulations s. 9(1) and (2)

**Relevant policy instruments and other references:** Directive on Privacy Practices and GC Guide on Personal information retention and disposal: Principles and best practices

**What "retention" means:** Only keep personal information for as long as you need it.

**Questions to consider:**

- For how long do you need to keep the personal information?
- Is there legal, regulatory or policy authority for retaining the information?
- Do you have a retention schedule for personal information that is in the institution's control?
- Is what form and format will information be retained?

**Risk example:**

- Personal information is retained longer than necessary for "just in case" scenarios
- Personal information is not retained long enough to allow individuals to access it
- Personal information retained for long periods may become inaccurate or out-of-date

**Mitigation example:**

- Establish minimum and maximum retention periods
- Have in place a records disposition authority (RDA) or appropriate interim measure
- Have in place a retention schedule
- Limit access to personal information that must be retained, but is no longer required
- Configure systems to delete personal information once the retention period has been reached or to make it inaccessible
- Conduct periodic audits or spot checks of your holdings to ensure personal information is being retained beyond established time periods

**Tip:** Keeping information longer than necessary may increase the risk and exposure of potential data breaches.

**Tip:** In assessing what is the appropriate retention period and whether it is time to dispose of personal information, consider the purpose for which it was collected.

- Establishing the purpose for having collected the personal information in the first place is generally helpful in assessing how long certain personal information should be retained. Consider the purpose in light of the relevant legal authorities, policy, and the institution's organizational of time thereafter – or another reasonable amount of time to allow for disputes or legislative requirements – to allow the individual to access that information in order to exercise their rights under the Privacy Act, if they so wish.
- If a third party personal information project would result in a prejudice for the concerned individual, or increase the risk and exposure to data breaches, the institution should safely dispose of it.

### Accuracy

**Relevant legal instrument:** Privacy Act s. 6(2)

**Relevant policy instrument:** Directive on Privacy Practices

**What "accuracy" means:** Make sure individuals' personal information is make a decision that affects them, or that you disclose to another government institution.

**Questions to consider:**

- How do you ensure data quality?
- Has an individuals request correction of their personal information?

**Risk example:**

- Personal information liable to individuals may be inaccurate, out-of-date or incomplete
- An institution may make decisions that directly affect an individual based on personal information that is inaccurate or incomplete
- Inaccurate, out-of-date or incomplete personal information may be shared with third parties
- Individuals may be unaware of their rights to correct their personal information held by an institution

**Mitigation example:**

- Periodically test the accuracy of information collected
- Have a process in place to correct inaccurate or out-of-date information
- Notify individuals of the procedures for correcting their personal information
- Notify individuals of the reasons for refusal and reasonable available to them for refusal their correction
- Allow individuals to add a statement to their personal information when their correction request has been refused

### Disclosure

**Relevant legal instrument:** Privacy Act s. 7, and s. 8 (1)

**Relevant policy instruments and other references:** Directive on Privacy Practices and GC Guide on Personal information retention and disposal: Principles and best practices

**What "disclosure" means:** Use care to prevent unauthorized access when disposing of personal information.

**Questions to consider:**

- How do you ensure proper disposal of?
- Are there issues in disposal of information in various formats (for example, paper, digital)
- Is the information covered by a RDA?

**Risk example:**

- Personal information is disposed of improperly and may be accessed without authorization
- Not all copies of information are disposed of

**Mitigation example:**

- Put in place procedures for secure disposal or destruction of personal information in the equipment of the institution, including computers and other devices
- Have in place an RDA or appropriate interim measure
- Ensure that personal information is disposed of in accordance with the RDA or other authorities
- When disposing of equipment or devices used for storing personal information (such as filing cabinets, computers, external drives, photocopiers and multi-function units), remove or delete any stored personal information

### Limiting use

**Relevant legal instrument:** Privacy Act s. 7

**Relevant policy instrument:** Directive on Privacy Practices

**What "limiting use" means:** Limit your use of individuals' personal information to your purpose identified at collection.

**Questions to consider:**

- What personal information will be used for and for what purpose?
- Is information used for purposes other than that it was collected?
  - Is it consistent purposes?
  - Is it consistent purposes?
- Is personal information being used for purposes not identified to the individual?
- Do you need to obtain consent for new purposes?

**Risk example:**

- Personal information provided for one purpose may be used inappropriately for a secondary purpose
- An employee may use personal information in a way that is contrary to the reasonable expectations of the individual

**Mitigation example:**

- Inform individuals of planned uses of their personal information
- Obtain consent for new uses of personal information, if required
- Establish appropriate processes for review, approval and monitoring of new uses of personal information

**Tip:** Interpret the definition of "consistent use" narrowly as it is an exception to seeking consent. This statement is interpreting with the square consistent value of the Privacy Act and the general principle that the statute protects. A consistent use" serious as it is one that has a reasonable and direct connection to the original purpose(s) for which the personal information was collected. It also means that the original purpose and the proposed purpose are so closely linked that an individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.

### Limiting disclosure

**Relevant legal instruments:** Privacy Act s. 8(1) and (2)

**Relevant policy instruments and other references:** Guidance on Preparing Information Sharing Agreements Involving Personal Information, Privacy Protocol for Information Sharing Agreements, Making Information Sharing Agreements Work! Checklist and Policy on Privacy Protection

**What "limiting disclosure" means:** Limit your sharing of individuals' personal information.

**Questions to consider:**

- What personal information will be disclosed, for what purpose and to whom?
- Do you have authority to share personal information, or the disclosure subject to an order?
- Have will information be shared?
- Are information sharing agreements in place with third parties with whom information is shared, and do they include clauses limiting further disclosure of information?
- Are there ways to organize that allow you to share the information in less way?

**Risk example:**

- Personal information could be shared without legal authority or consent
- Association, knowledge or consent data could be shared with third parties
- Third parties may inappropriately protect personal information that has been shared
- Personal information may be disclosed to third parties without a clear purpose

**Mitigation example:**

- Inform individuals of planned disclosures of their personal information
- Obtain consent for new disclosures of personal information, if required
- Establish appropriate processes for seeking consent, as necessary
- Include robust privacy and security requirements in agreements with third parties with whom personal information is shared
- Use appropriate safeguards to protect personal information in transit

### Safeguards

**Relevant legal instruments:** Privacy Act s. 7

**Relevant policy instruments and other references:** Policy on Government Security, Directive on Security Management, Operational Security Standard: Management of Information Technology Security, GC Guideline on Privacy Practices and Guideline for Privacy Breaches

**What "safeguards" means:** Take steps to secure personal information from unauthorized access, use or disclosure.

**Questions to consider:**

- What security and access controls will protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification whether in paper or in text?
- Do your staff understand how to protect personal information in a more sensitive?
- Do your staff understand how to protect personal information?
- Does personal information travel or reside outside of Canada?

**Risk example:**

- Staff may not be used to know more gain access to personal information
- An institution may not be able to detect unauthorized access to personal information
- Sensitivities information may be identifiable when combined with other information, including personal information

**Mitigation example:**

- Use appropriate physical safeguards (restricted access and locks) institutional safeguards (training and security clearances) and technical safeguards (audits and encryption) to protect personal information
- Use a variety of safeguards, depending on the information's sensitivity, amount, distribution, format, and storage medium
- Use pseudonyms or de-identified information, where possible
- Have in place a process for reporting privacy breaches
- Have in place a breach response procedure as well as measures to detect a breach
- Include robust privacy and security requirements in agreements with third parties with whom information is shared
- Conduct appropriate security assessments
- Conduct ongoing testing of safeguards to ensure they are functioning appropriately

**Tip:** The most effective privacy safeguard is not to collect personal information in the first place if you don't need it.

**Tip:** Part of a PIA is to identify the most appropriate level of security in specific circumstances, not the strongest information security possible.

### Openness

**Relevant legal instruments:** Privacy Act s. 4, 5(2) and 11

**Relevant policy instruments:** Directive on Privacy Practices and Policy on Privacy Protection

**What "openness" means:** Be open, clear and straightforward about your handling of personal information.

**Questions to consider:**

- Are individuals informed of:
  - Why personal information is being sought?
  - For what purpose will with what purpose?
  - Its consequences for not providing the information?
  - Its use for secondary purposes?
  - Its for how or other reasons?
  - Its disclosure to other government institutions?
  - Do they informed (for example, signage, forms, privacy notice, Personal information Bank (PIB)?

**Risk example:**

- Individuals may be unaware of the collection, use and disclosure of their personal information
- Notices may not be easily accessible to all individuals
- Notices may be difficult to understand, or not in plain language

**Mitigation example:**

- Make information about your personal information handling practices readily available and easy to understand
- Use plain language, avoid jargon, a variety of ways and ensure it is consistent across formats (for example, signage, written or verbal notice)
- Whenever possible, notify individuals of your practices at or before the time of collection
- Make information available in official languages

**Tip:** Institutions are required to describe in their annual reports to Parliament the uses of personal information to better institution, as appropriate. For example, some summaries of Statistics Canada surveys, or Canada Revenue Agency tax information, may be of interest to Canadians and other human, or these, for information that contains sensitive information. Specifically, consent is not required if the information is used for statistical or research purposes, but only if the information will not be used in any way that affects the individual to whom it relates, and the results will not be released in a form that would permit the identification of individuals. If information is not an objective, the results must be in the form of consent.

Refer to s. 7 and 8 of the Privacy Act and the Directive on Privacy Practices for more information.

**Tip:** The federal government publication Information about programs and information holdings is intended to provide individuals with an index of personal information held by government institutions subject to the Privacy Act.

### Individual access

**Relevant legal instruments:** Privacy Act s. 4, 5(2) and 12

**Relevant policy instruments:** Directive on Personal Information Requests and Correction of Personal Information and Policy on Privacy Protection

**What "individual access" means:** Give citizens, permanent residents and those present in Canada access to the information you hold about them and correct, if requested.

**Questions to consider:**

- What is the process for assessing and responding to requests for access to and correction of personal information in a timely manner?
- Do you have adequate oversight of their rights of access and correction?

**Risk example:**

- Delays in processing requests may be delayed in responding to requests for access to personal information, or requests for correction of personal information
- Individuals may be unaware of their right to access or correct their personal information held by an institution

**Mitigation example:**

- Develop an document a process for responding to access and correction requests
- Inform individuals of their right to request access and correction of their personal information
- Ensure staff are aware of an individual's personal information can be retrieved without unnecessary difficulty
- Verify the identity of individuals requesting access to their personal information
- Establish a process for notifying third parties to whom personal information has been disclosed of a correction
- Allow individuals to add a statement to their personal information when their access or correction request has been refused
- Establish a process to inform third parties to whom personal information has been shared

**Tip:** Complaints to providing access to personal information should be interpreted as narrowly as possible.

### Risk mitigation plan

Now that you have identified the privacy risks associated with your institutional program or activity, you should develop a risk mitigation plan. Risk management approaches and processes will be specific to your institution and will depend on its:

- mandate
- culture
- risk appetite
- institutional risk culture
- risk management
- current and stakeholder interests

The risk tolerance you take into account making controls and risk responses is referred to as the "residual" risk. Residual risk is the risk that remains after you have implemented your risk mitigation measures. It is defined as the "residual" risk level. The risk tolerance level that you choose to accept is not the "residual" risk, but the policy and procedure and training program and as such function to reduce it. Residual risk is the risk that remains after you have implemented your risk mitigation measures.

Risk tolerance is the level of risk that an organization is willing to accept. Risk tolerance is a matter of risk appetite and complexity. However, even highly conservative risk tolerance organizations may be prepared to accept. There are some risks that are beyond their control, such as those arising from natural disasters or pandemics. Other risks may be accepted because the cost of eliminating or reducing them may be prohibitively expensive. Institutions should consider integrating privacy risk management into their broader risk management framework and plans.

### Action plan

There is little point investing time or resources in a PIA process and then failing to take action. An action plan can help you track and manage the decisions you've made as a result of the PIA process. Your action plan should include the following information for each privacy risk you have identified:

- area of the institution or particular member(s) of the project team responsible for its implementation
- estimated timeline for completion

You can update the plan as measures are implemented so that your progress can be tracked.

### Drafting phase

Once you have assessed and integrated your program or activity's risks, you will need to document the results of your PIA in a formal report. The PIA report should include a description of the program or activity that could be involved in your PIA report. You are encouraged to include additional information, as appropriate, in the PIA report can show are no needed.

PIA report level previews

- No specific
- Brief (one-page) level use of acronyms
- Recursive – "more complex, fewer words"
- No action oriented – what do you plan to do?
- Use of "plain language" and "plain language"
- Organized and easy to navigate and structure the area to navigate or repeat material
- Use of "plain language" and "plain language" and "plain language" and "plain language"

### Approval phase

Next, you will need to obtain internal approvals in accordance with the Directive on Privacy Impact Assessment. Depending on the nature and scope of your program or activity, senior officials responsible for your program and your integrated executive can judge. It is an institutional responsibility to ensure that the privacy risks are properly managed.

**Tip:** The PIA can be a separate, standalone or sign off of PIAs or an government programs or activities. Institutions may choose to use the PIA with other institutions, and provinces, and provide recommendations where one identifies additional risks or gaps.

### Reporting phase

Officially requires that institutions make select sections of the PIA report publicly available (as per the Directive on Privacy Impact Assessment). Public reporting allows individuals to learn about of the new or modified programs or activities that may affect their privacy and how their privacy is protected.

PIA reports, or their summaries, should be clear, unequivocal, and understandable and written in general not especially once they are publicly available. Institutions should post, at a minimum, summaries of their PIA reports on their institutional Web sites. Institutions should post PIA reports on the Web site of the Treasury Board Secretariat and Information Commissioner of Canada. The Treasury Board Secretariat and Information Commissioner of Canada protect breach such as commercial confidentiality, national security, personal information or legal privilege and jurisdictions.

### Review phase

Institutions should have an ongoing process that does not stop with the approval of the PIA. You should assess privacy controls, risks, etc. regularly as the environment changes. Institutions should review PIAs and should assess whether the measures implemented are still sufficient to the PIA or attach a short addendum. In other cases, you should review the relevant changes and analyze the implications of the changes. A change in substantial and should is significant two privacy impact, but were not considered in the PIA, you should update the PIA and post the updated PIA on the Web site. Institutions should review PIAs.

## Acknowledgements


This Guide is intended as a tool to assist government institutions when determining how best to achieve compliance with the Privacy Act. Nothing in this Guide should be considered binding in law, or in any way fettering the discretion of the Privacy Commissioner in the performance of his duties and functions. We wish to thank the OPC complaint under the Privacy Act on the understanding of an audit or review by the OPC under the Act.


## Footnotes

1. According to the Office of the Privacy Commissioner's 2013-14 Survey of Canadians on Privacy.
2. For more information see the TBS's Directive on Automated Decision-Making.
3. Sections 7 and 8 of the Privacy Act place requirement restrictions to use and disclosure of personal information. Section 8 provides specified purposes in order to protect personal information. Requirements for information collected requires that institutions comply with those provisions.




**About the OPC**

The Privacy Commissioner of Canada oversees compliance with the Privacy Act and promotes privacy rights.

**OPC news**

Get updates on the Commissioner's activities, decisions, and participation.

Contact us for information about subscribing.

**Your privacy**

**We respect your privacy**

Learn how we manage your personal information and cookies, and more about your privacy rights and how to file a complaint with the Privacy Commissioner of Canada.

**Contact us**

Find ways to reach us and learn about the ways we can help.