A Guide for **Businesses** and **Organizations**

PRIVACY TOOLKIT

Canada's *Personal Information Protection and Electronic Documents Act*

Office of the
Privacy Commissioner
of Canada

For more information, contact:

Office of the Privacy Commissioner of Canada
30 Victoria Street, 1st floor
Gatineau, QC
K1A 1H3

Telephone: (819) 994-5444
Toll-free: 1-800-282-1376
Fax: (819) 994-5424

Website: www.priv.gc.ca
Follow us on Twitter: @privacyprivee

IP54-58/2014E-PDF
ISBN: 978-1-100-23366-6

Updated March 2014

This guide deals only with Part 1 of the Act. All references to the Act in this document refer only to Part 1. Parts 2 to 5 of the Act concern the use of electronic documents and signatures as legal alternatives to original documents and signatures. For information on these, please contact the Department of Justice.

TO LEARN MORE

This document highlights a number of other resources which provide more detailed information about how organizations can meet their obligations under PIPEDA. To link to these documents, please see the electronic version of this guide on the Office of the Privacy Commissioner of Canada website at www.priv.gc.ca.

TABLE OF CONTENTS

OVERVIEW

The Office of the Privacy Commissioner of Canada has prepared this guide to help organizations fulfill their responsibilities under the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Individuals will appreciate doing business with organizations that demonstrate a respect for their privacy rights, which can ultimately lead to a competitive advantage for businesses. Organizations can see this as an opportunity to review and improve their personal information handling practices.

ROLE OF THE PRIVACY COMMISSIONER OF CANADA

The Privacy Commissioner of Canada is responsible for oversight of both the *Privacy Act* and Part 1 of PIPEDA. These acts protect personal information entrusted to federal institutions and commercial organizations, respectively.

As an Agent of Parliament, the Commissioner reports directly to the House of Commons and to the Senate, not to the government of the day. This independence ensures impartiality and open-mindedness in exercising his or her role as an ombudsman for privacy matters.

While the Commissioner protects individual rights, he or she is also an advocate for the fair information principles that form the foundation of PIPEDA.

The Commissioner's thorough investigations and impartiality protect both individual rights and the organization against unfair accusations.

The Commissioner promotes the purposes of the Act through public education and awareness initiatives, research, reporting, and consultation and agreements.

PIPEDA also requires the Commissioner to undertake and publish research about protecting personal information so as to increase knowledge and improve compliance with the Act's fair information principles. The Commissioner may conduct independent research on privacy issues in conjunction with academic or other researchers. He or she may also provide grants and contributions for academic or other research on privacy issues.

The Commissioner reports annually to Parliament on privacy issues.

PIPEDA IN BRIEF

Organizations covered by the Act must obtain an individual's consent when they collect, use or disclose the individual's personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by appropriate safeguards.

Under PIPEDA, the definition of organization includes an association, a partnership, a person or a trade union.

HOW THE ACT APPLIES

PIPEDA applies to the collection, use or disclosure of personal information in the course of a commercial activity.

A commercial activity is defined as any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fund-raising lists.

The federal government may exempt from PIPEDA organizations and/or activities in provinces that have adopted substantially similar privacy legislation. To date, Quebec, British Columbia and Alberta have adopted private sector legislation deemed substantially similar to the federal law. As well, Ontario, New Brunswick and Newfoundland and Labrador have adopted substantially similar legislation with respect to personal health information.

Even in those provinces which have adopted substantially similar privacy legislation, PIPEDA continues to apply in all interprovincial and international transactions by all organizations subject to the Act in the course of their commercial activities.

As well, PIPEDA continues to apply in those provinces to federally regulated organizations – "federal works, undertakings or businesses" – such as banks, telecommunications and transportation companies.

WHAT IS A "FEDERAL WORK, UNDERTAKING, OR BUSINESS"?

This term includes "any work, undertaking or business that is under the legislative authority of Parliament". While most federally regulated organizations would be captured under this definition, not all these types of organizations are federal works. For instance, insurance companies and credit unions may be subject to some federal regulation, but are considered to be within provincial jurisdiction under the Constitution and are not federal works for the purposes of the Act. The Act defines what constitutes a federal work, undertaking or business subject to Part 1 to include:

- airports, aircraft or airlines
- banks
- inter-provincial or international transportation by land or water
- telecommunications
- offshore drilling operations
- radio and television broadcasting

Note that this is not an exhaustive list of "federal works, undertakings and businesses." The fact that your company is federally incorporated does not necessarily mean that it is a federal work, undertaking or business. If your company is subject to any part of the Canada Labour Code, it may be a federal work, undertaking or business.

WHAT IS "PERSONAL INFORMATION"?

Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as:

- age, name, ID numbers, income, ethnic origin, or blood type;
- opinions, evaluations, comments, social status, or disciplinary actions; and
- employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs.)

WHAT IS *NOT* COVERED BY PIPEDA?

There are some instances where PIPEDA does not apply. Some examples include:

- Personal information collected, used or disclosed by federal government organizations listed under the *Privacy Act*
- Provincial or territorial governments and their agents
- An employee's name, title, business address or telephone number
- An individual's collection, use or disclosure of personal information strictly for personal purposes (e.g. personal greeting card list)
- An organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes
- Employee information – except in the federally-regulated sector

COMPLAINTS TO THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

An individual may complain to the organization in question or to the Office of the Privacy Commissioner of Canada about any alleged breaches of the law.

The Commissioner may also initiate a complaint, if there are reasonable grounds.

Whenever possible, the Office of the Privacy Commissioner of Canada seeks to resolve disputes through investigation, persuasion, mediation and conciliation. Ideally this approach to resolving disputes can be less intimidating to complainants and less costly to business than recourse to the courts.

In some cases, where a complaint involves a concern that could potentially be resolved quickly, the complaint is referred to an early resolution officer.

The early resolution officer works with both the complainant and the respondent organization to resolve a complaint. In some cases, an issue that would have taken months to resolve through the official complaint investigation process can be concluded in a matter of days.

If a resolution cannot be found, the complaint is then investigated and ultimately a report of findings is issued by the Office of the Privacy Commissioner of Canada.

The Commissioner makes recommendations, not orders. However there is provision in PIPEDA that allows complainants or the Privacy Commissioner to apply to the Federal Court for a hearing in certain cases.

The Court may order an organization to change its practices and/or award damages to a complainant, including damages for any humiliation suffered.

The Commissioner may make public any information about an organization's personal information handling practices, if he or she considers it in the public interest to do so.

AUDITS

The Commissioner may, with reasonable grounds, audit the personal information management practices of an organization.

OFFENCES

Under PIPEDA, it is an offence to:

- destroy personal information that an individual has requested;
- retaliate against an employee who has complained to the Commissioner or who refuses to contravene Sections 5 to 10 of the Act; or
- obstruct a complaint investigation or an audit by the Commissioner or his or her delegate.

ORGANIZATIONS' RESPONSIBILITIES UNDER THE ACT

Organizations must follow a code for the protection of personal information, which is included in the Act as Schedule 1. The code was developed by business, consumers, academics and government under the auspices of the Canadian Standards Association.

The 10 principles that businesses must follow are:

1. Accountability
2. Identifying purposes
3. Consent
4. Limiting collection
5. Limiting use, disclosure, and retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual access
10. Challenging compliance

These principles are described in detail in the following sections of this guide.

TO LEARN MORE

For more detailed information, please see the following documents on our website:

About the Office of the Privacy Commissioner of Canada

Legal information related to the Personal Information Protection and Electronic Documents Act

PIPEDA Self-Assessment Tool

Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's *Personal Information Protection Acts*

The Application of the *Personal Information Protection and Electronic Documents Act* to Charitable and Non-Profit Organizations

FAIR INFORMATION PRINCIPLES

Schedule 1 of PIPEDA sets out 10 principles of fair information practices, which form the ground rules for the collection, use and disclosure of personal information, as well as for providing access to personal information. These principles give individuals control over how their personal information is handled in the private sector.

However, organizations should note that in addition to the principles set out under Schedule 1 of PIPEDA, the Act contains an overriding obligation that any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider are appropriate in the circumstances. This overarching standard of appropriateness of purposes continues to apply independent from the provisions of Schedule 1 of the Act.

An organization is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. Additionally, care in collecting, using and disclosing personal information is essential to continued consumer confidence and good will.

This section sets out the responsibilities for each of the 10 fair information principles under Schedule 1. It outlines how to fulfill these responsibilities and offers some tips.

1. BE ACCOUNTABLE

Your responsibilities

- Comply with all 10 of the principles of Schedule 1.
- Appoint an individual (or individuals) to be responsible for your organization's compliance.
- Protect all personal information held by your organization or transferred to a third party for processing.
- Develop and implement personal information policies and practices.

How to fulfill these responsibilities

Develop a privacy management program. As part of this program:

- Give your designated privacy official senior management support and the authority to intervene on privacy issues relating to any of your organization's operations.
- Communicate the name or title of this individual internally and externally (e.g. on websites and in publications).
- Analyze and document all personal information handling practices including ongoing activities and new initiatives, using the following checklist to ensure that they meet fair information practices:
  - ☐ What personal information do we collect and is it sensitive? (Sensitive information may require extra protection.)
  - ☐ Why do we collect it?
  - ☐ How do we collect it?
  - ☐ What do we use it for?
  - ☐ Where do we keep it?
  - ☐ How is it secured?
  - ☐ Who has access to or uses it?
  - ☐ To whom is it disclosed?
  - ☐ When is it disposed of?
- Develop, document and implement policies and procedures to protect personal information:
  - ☐ define the purposes of its collection
  - ☐ obtain consent
  - ☐ limit its collection, use and disclosure
  - ☐ ensure information is correct, complete and current
  - ☐ ensure adequate security measures
  - ☐ develop or update a retention and destruction timetable

- develop and implement policies and procedures to respond to access requests as well as inquiries and complaints
- develop, document and implement breach and incident management protocols
- conduct risk assessments
- develop, document and implement appropriate service provider management practices
- develop, document and deliver appropriate privacy training for employees

- Regularly assess your privacy management program and address any shortcomings.
- Be prepared to demonstrate that you have a privacy management program in place and that it is being followed.
- Make information available explaining your privacy policies and procedures to customers (e.g. in brochures and on websites).

TIPS

Train your front-line and management staff and keep them informed, so they can answer the following questions:

- How do I respond to public inquiries regarding our organization's privacy policies?
- What is consent? When and how is it to be obtained?
- How do I recognize and process requests for access to personal information?
- To whom should I refer complaints about privacy matters?
- What are the ongoing activities and new initiatives relating to the protection of personal information at our organization?

Tips for transferring personal information to third parties

When transferring personal information to third parties, your contract with them should ensure that they:

- Name a person to handle all privacy aspects of the contract.
- Limit use of the personal information to the purposes specified to fulfil the contract.
- Limit disclosure of the information to what is authorized by your organization or required by law.
- Refer any people looking for access to their personal information to your organization.
- Return or dispose of the transferred information upon completion of the contract.
- Use appropriate security measures to protect the personal information.
- Allow your organization to audit the third party's compliance with the contract as necessary.

TO LEARN MORE

For more detailed information, please see the following documents on our website:

Getting Accountability Right with a Privacy Management Program

Interpretation Bulletin: Accountability

Interpretation Bulletin: Personal Information

Build a Privacy Plan for your Business

PIPEDA Self-Assessment Tool

Guidelines for Processing Personal Data Across Borders

Privacy and Your Business: Privacy Breach Handbook

Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency LINK TBD

2. IDENTIFY THE PURPOSE

Your organization must identify the reasons for collecting personal information before or at the time of collection.

Your responsibilities

- Before or when any personal information is collected, identify why it is needed and how it will be used.
- Document why the information is collected.
- Inform the individual from whom the information is collected why it is needed.
- Identify any new purpose for the information and obtain the individual's consent before using it.

How to fulfill these responsibilities

- Review your personal information holdings to ensure they are all required for a specific purpose.
- Notify the individual, either orally or in writing, of these purposes.
- Record all identified purposes and obtained consents for easy reference in case an individual requests an account of such information.
- Ensure that these purposes are limited to what a reasonable person would expect under the circumstances.

TIPS

- Define your purposes for collecting data as clearly and narrowly as possible so the individual can understand how the information will be used or disclosed.
- Avoid overly broad purposes as they may conflict with the knowledge and consent principle.
- Examples of purposes include:
  - opening an account
  - verifying creditworthiness
  - providing benefits to employees
  - processing a magazine subscription
  - sending out association membership information
  - guaranteeing a travel reservation
  - identifying customer preferences
  - establishing customer eligibility for special offers or discounts.

3. OBTAIN INFORMED CONSENT

Your responsibilities

- Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data.
- Obtain the individual's consent before or at the time of collection, as well as when a new use of their personal information is identified.

How to fulfill these responsibilities

- Obtain informed consent from the individual whose personal information is collected, used or disclosed.
- Explain how the information will be used and with whom it will be shared. This explanation should be clear, comprehensive, and easy to find. Retain proof that consent has been obtained.
- Never obtain consent by deceptive means.
- Do not deny a product or service to an individual who fails to consent to the collection, use or disclosure of information *beyond* that required to fulfill an explicitly specified and legitimate purpose.
- Explain to individuals the implications of withdrawing their consent.
- Ensure that employees collecting personal information are able to answer individuals' questions about why they are being asked for this information.

UNDERSTANDING KNOWLEDGE AND CONSENT

Knowledge and consent means informed and voluntary agreement with what is being done or proposed. Consent is meaningful when individuals understand what the organization is doing with their information. Consent can be either express or implied. Express consent is given explicitly, either orally, in writing, or through a specific online action, such as clicking on "I agree". Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual. Consent does not waive an organization's other responsibilities under PIPEDA, such as overall accountability, safeguards, and having a reasonable purpose for processing personal information.

TIPS

- Consent is normally obtained from the individual whose personal information is collected, used or disclosed.
- For an individual who is a minor, seriously ill, or mentally incapacitated, consent may be obtained from a legal guardian, or person having power of attorney.
- In order for individuals to understand what they are consenting to, organizations should be transparent about their information management practices. Privacy policies and consent statements should:
  - be easy to find
  - use clear and straightforward language
  - not use blanket categories for purposes, uses and disclosures
  - be specific as possible about which organizations handle the information
  - explain practices that an individual might not reasonably expect, such as disclosures to third parties
- Online, privacy policies should be supplemented by other types of privacy disclosures, such as just-in-time notifications, and should provide privacy explanations at key points in the user experience.
- Consent can be obtained in person, by phone, by mail, or online.
- The form of consent should take into consideration:
  - reasonable expectations of the individual
  - circumstances surrounding the collection
  - sensitivity of the information involved.
- Express, or opt-in, consent should be used whenever possible and in all cases when the personal information is considered sensitive. Relying on express consent protects both the individual and the organization.
- When using opt-out consent, the organization should establish a convenient procedure for withdrawing consent, and the opt-out should take effect immediately.

TO LEARN MORE

For more detailed information, please see the following documents on our website:

Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency

PIPEDA and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

Fact Sheet - Determining the appropriate form of consent under the Personal Information Protection and Electronic Documents Act

Exceptions to the Consent Principle

There are a number of specific exceptions to the requirements to obtain knowledge and consent for the collection, use or disclosure of personal information.

Organizations may **collect** personal information without the individual's knowledge or consent only:

- if it is clearly in the individual's interests and consent is not available in a timely way;
- if knowledge and consent would compromise the availability or accuracy of the information and collection is required to investigate a breach of an agreement or contravention of a federal or provincial law;
- for journalistic, artistic or literary purposes;
- if it is publicly available as specified in the regulations.

Organizations may **use** personal information without the individual's knowledge or consent only:

- if the organization has reasonable grounds to believe the information could be useful when investigating a contravention of a federal, provincial or foreign law and the information is used for that investigation;
- for an emergency that threatens an individual's life, health or security;
- for statistical or scholarly study or research (the organization must notify the Privacy Commissioner of Canada before using the information);
- if it is publicly available as specified in the regulations;

- if the use is clearly in the individual's interest and consent is not available in a timely way; or
- if knowledge and consent would compromise the availability or accuracy of the information and collection was required to investigate a breach of an agreement or contravention of a federal or provincial law.

Organizations may **disclose** personal information without the individual's knowledge or consent only:

- to a lawyer representing the organization;
- to collect a debt the individual owes to the organization;
- to comply with a subpoena, a warrant or an order made by a court or other body with appropriate jurisdiction;
- to the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) as required by the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*;
- to a government institution that has requested the information, identified its lawful authority to obtain the information, and indicates that disclosure is for the purpose of enforcing, carrying out an investigation, or gathering intelligence relating to any federal, provincial or foreign law; or suspects that the information relates to national security, the defence of Canada or the conduct of international affairs; or is for the purpose of administering any federal or provincial law;
- to an investigative body named in the Regulations of the Act or government institution on the organization's initiative when the organization has reasonable grounds to believe that the information concerns a breach of an agreement, or a contravention of a federal, provincial, or foreign law, or suspects the information relates to national security, the defence of Canada or the conduct of international affairs;
- if made by an investigative body for the purposes related to the investigation of a breach of an agreement or a contravention of a federal or provincial law;
- in an emergency threatening an individual's life, health, or security (the organization must inform the individual of the disclosure);
- for statistical, scholarly study or research (the organization must notify the Privacy Commissioner before disclosing the information);
- to an archival institution;
- 20 years after the individual's death or 100 years after the record was created;
- if it is publicly available as specified in the regulations; or
- if required by law.

4. LIMIT COLLECTION

Your responsibilities

- Do not collect personal information indiscriminately.
- Do not deceive or mislead individuals about the reasons for collecting personal information.

How to fulfill these responsibilities

- Limit the amount and type of the information gathered to what is necessary for the identified purposes.
- Identify the kind of personal information you collect in your information-handling policies and practices.
- Ensure that staff members can explain why the information is needed.

TIPS

- By reducing the amount of information gathered, you can lower the cost of collecting, storing, retaining and ultimately archiving data.
- Collecting less information also reduces the risk of inappropriate uses and disclosures.

TO LEARN MORE

For more detailed information, please see the following documents on our website:

Best Practices for the use of Social Insurance Numbers in the private sector

Collection of Driver's Licence Numbers Under Private Sector Privacy Legislation – A Guide for Retailers

Photo Identification Guidance

Guidelines for Recording Customer Telephone Calls

Guidelines for Overt Video Surveillance in the Private Sector

Guidance on Covert Video Surveillance in the Private Sector

Guidelines for Identification and Authentication

5. LIMIT USE, DISCLOSURE AND RETENTION

Your responsibilities

- Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act.
- Keep personal information only as long as necessary to satisfy the purposes.
- Put guidelines and procedures in place for retaining and destroying personal information.
- Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.
- Destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.

How to fulfill these responsibilities

- Document any new purpose for the use of personal information.
- Institute maximum and minimum retention periods that take into account any legal requirements or restrictions and redress mechanisms.
- Dispose of information that does not have a specific purpose or no longer fulfills its intended purpose.
- Dispose of personal information in a way that prevents a privacy breach. Shredding paper files or deleting electronic records are ideal.
- Before disposing of electronic devices such as computers, photocopiers and cellphones, ensure that all personal information is fully deleted.
- Establish policies setting out the types of information that need to be updated. An organization can reasonably expect an individual to provide updated information in certain circumstances (e.g. change of address for a magazine subscription).

TIPS

- It may be less onerous and complicated to destroy or erase information than to make personal information anonymous.
- Conduct regular reviews to help determine whether information is still required. Establish a retention schedule to make this easier.

TO LEARN MORE

For more detailed information, please see the following document on our website:

PIPEDA and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

6. BE ACCURATE

Your responsibilities

- Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

How to fulfill these responsibilities

- Keep personal information as accurate, complete and up to date as necessary, taking into account its use and the interests of the individual.
- Keep frequently used information accurate and up to date unless there are clearly set out limits to this requirement.

TIPS

- One way to determine whether information needs to be updated is to ask whether the use or disclosure of out of date or incomplete information would adversely affect the individual.
- Apply the following checklist for accuracy:
  - List specific items of personal information required to provide a service.
  - List the location where all related personal information can be retrieved.
  - Record the date when the personal information was obtained or updated.
  - Record the steps taken to verify accuracy, completeness and timeliness of the information. This may require reviewing your records or communicating with the client.

7. USE APPROPRIATE SAFEGUARDS

Your responsibilities

- Protect personal information against loss or theft.
- Safeguard the information from unauthorized access, disclosure, copying, use or modification.
- Protect personal information regardless of the format in which it is held.

Note: PIPEDA does not specify particular security safeguards that must be used. Rather, the onus is on organizations to ensure that personal information is adequately protected.

How to fulfill these responsibilities

- Develop and implement a security policy to protect personal information.
- Use appropriate security safeguards to provide necessary protection:
  - physical measures (locked filing cabinets, restricting access to offices, alarm systems)
  - technological tools (passwords, encryption, firewalls)
  - organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, agreements).
- Ensure that you regularly review security safeguards to ensure they are up-to-date and known vulnerabilities have been addressed.
- Make your employees aware of the importance of maintaining the security and confidentiality of personal information.
- Ensure staff awareness by holding regular staff training on security safeguards.
- The following factors should be considered in selecting appropriate safeguards:
  - sensitivity of the information
  - amount of information
  - extent of distribution
  - format of the information (electronic, paper, etc.)
  - type of storage.
- Review and update security measures regularly.

TIPS

- Make sure personal information that has no relevance to the transaction is either removed or blocked out when providing copies of information to others.
- Keep sensitive information files in a secure area or computer system and limit access to individuals on a "need-to-know" basis only.

TO LEARN MORE

For more detailed information, please see the following documents on our website:

Securing Personal Information: A Self-Assessment Tool for Organizations

Guidelines for Identification and Authentication

WHEN THINGS GO WRONG

A privacy breach occurs when there is unauthorized access to, or disclosure of personal information. The Office of the Privacy Commissioner of Canada has developed a number of resources to help organizations to take appropriate steps when a breach happens. Please see:

Information about privacy breaches and how to respond

8. BE OPEN

Your responsibilities

- Inform customers, clients and employees that you have policies and practices for the management of personal information.
- Make these policies and practices understandable and easily available.

How to fulfill these responsibilities

- Ensure front-line staff is familiar with the procedures for responding to individual inquiries.
- Make the following available:
  - name or title and address of the person who is accountable for your organization's privacy policies and practices
  - name or title and address of the person to whom access requests should be sent
  - how an individual can gain access to his or her personal information
  - how an individual can complain to your organization
  - brochures or other information that explain your organization's policies, standards or codes
  - a description of what personal information is made available to other organizations (including subsidiaries) and why it is disclosed.

TIPS

- Information about these policies and practices should be made available in person, in writing, by telephone, in publications or on your organization's website. The information presented should be consistent, regardless of the format.

TO LEARN MORE

For more detailed information, please see the following document on our website:

Ten Tips for a Better Online Privacy Policy and Improved Privacy Practice Transparency

9. GIVE INDIVIDUALS ACCESS

Generally speaking, individuals have a right to access the personal information that an organization holds about them.

Your responsibilities

- When requested, inform individuals if you have any personal information about them.
- Explain how it is or has been used and provide a list of any organizations to which it has been disclosed.
- Give individuals access to their information.
- Correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient.
- Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in Section 9 of the Act. (See Exceptions to the Access Principle on page 24.)
- An organization should note any disagreement on the file and advise third parties where appropriate.

How to fulfill these responsibilities

- Provide any help the individual needs to prepare a request for access to personal information.
- Your organization may ask the individual to supply enough information to enable you to account for the existence, use and disclosure of personal information.
- Respond to the request as quickly as possible, and no later than 30 days after receipt of the request.
- The normal 30-day response time limit may be extended for a maximum of 30 additional days, according to specific criteria set out at Subsection 8(4) of the Act:

  - if responding to the request within the original 30 days would unreasonably interfere with activities of your organization
  - if additional time is necessary to conduct consultations
  - if additional time is necessary to convert personal information to an alternate format.

- If your organization extends the time, you must notify the individual making the request within 30 days of receiving the request, and of his or her right to complain to the Privacy Commissioner of Canada.
- Give access at minimal or no cost to the individual.
- Notify the individual of the approximate costs before processing the request and confirm that the individual still wants to proceed with the request.
- Make sure the requested information is understandable. Explain acronyms, abbreviations and codes.
- Send any information that has been amended, where appropriate, to any third parties that have access to the information.
- Inform the individual in writing when refusing to give access, setting out the reasons and any recourse available.

TIPS

- Keep a record of where the information can be found to make retrieval easier.
- Ensure you conduct a thorough search in all of the places where personal information may be stored – both physically and electronically.
- Never disclose personal information unless you are sure of the identity of the requestor and that person's right of access.
- Record the date of receipt of the request for the information.
- Ensure that staff members know how to identify an access request and to whom it should be referred within the organization.

TO LEARN MORE

For more detailed information, please see the following documents on our website:

Fact Sheet - Accessing Personal Information under the Personal Information Protection and Electronic Documents Act

PIPEDA and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

EXCEPTIONS TO THE ACCESS PRINCIPLE

While organizations have a general obligation under PIPEDA to provide access to personal information upon request, there are specific exceptions to this obligation.

PIPEDA sets out both mandatory and discretionary exceptions to providing access to personal information upon request.

In terms of mandatory exceptions, organizations **must** refuse an individual access to personal information:

- if it would reveal personal information about another individual* unless there is consent or a life-threatening situation; or
- if an individual requests that he or she be informed of information disclosed to a government institution in certain specified cases, or for access to the information itself, and the government institution objects to the institution complying with the access request. In such cases, the organization must refuse the request and notify the Privacy Commissioner of Canada. As well, the organization cannot inform the individual of the disclosure to the government institution, that the institution was notified of the request, or that the Privacy Commissioner of Canada was notified of the refusal.

In terms of discretionary exceptions, organizations **may** refuse access to personal information if the information:

- is protected by solicitor-client privilege;
- would reveal confidential commercial information;*
- would reasonably be expected to harm an individual's life or security;*
- was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner of Canada must be notified);
- was generated in the course of a formal dispute resolution process; or
- was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or a related investigation.

* If this information can be severed, the organization must release the remaining information.

10. PROVIDE RECOURSE

Your responsibilities

- Develop simple and easily accessible complaint procedures.
- Inform complainants of their avenues of recourse. These include your organization's own complaint procedures, those of industry associations, regulatory bodies and the Office of the Privacy Commissioner of Canada.
- Investigate all complaints received.
- Take appropriate measures to correct information handling practices and policies.

How to fulfill these responsibilities

- Record the date a complaint is received and the nature of the complaint (e.g. delays in responding to a request, incomplete or inaccurate responses, or improper collection, use, disclosure or retention).
- Acknowledge receipt of the complaint promptly.
- Contact the individual to clarify the complaint, if necessary.
- Assign the matter to a person with the skills necessary to review it fairly and impartially and provide that individual with access to all relevant records, employees or others who handled the personal information or access request.
- Notify individuals of the outcome of investigations clearly and promptly, informing them of any relevant steps taken.
- Correct any inaccurate personal information or modify policies and procedures based on the outcome of complaint, and ensure that employees in the organization are aware of any changes to these policies and procedures.

TIPS

- Ensure that staff members are aware of policies and procedures for complaints, and to whom these complaints should be referred within the organization.
- Record all decisions to ensure consistency in applying the Act.
- Handling a complaint fairly and appropriately may help to preserve or restore the individual's confidence in your organization.

TO LEARN MORE

For more detailed information, please see the following documents on our website:

Getting Accountability Right with a Privacy Management Program

Ten tips for avoiding complaints to the OPC

COMPLAINTS TO THE PRIVACY COMMISSIONER OF CANADA

TYPES OF COMPLAINTS

An individual may complain to the Commissioner about any matter specified in Sections 5 to10 of the Act or in the recommendations or obligations set out in Schedule 1.

If the Commissioner is satisfied that there are reasonable grounds to investigate a matter, the Commissioner may initiate a complaint against an organization pursuant to subsection 11(2).

When assessing whether there are reasonable grounds to initiate a complaint, the Commissioner will determine whether there is credible evidence that supports a serious possibility that an investigation would disclose a contravention or intended contravention of the Act.

TIME LIMITS

There is no time limit for filing most types of complaints. That being said, the Commissioner may decline to investigate a complaint if he or she is of the opinion that it was not filed within a reasonable period.

The only exception is a complaint that access to personal information has been denied. In this case, the complaint must be made within six months after the organization's refusal to provide the information, or after the expiry of the time limit for responding to the request. However, the Commissioner may extend the time limit for an access complaint.

The Commissioner has one year from the date of the complaint to prepare a report.

HOW DOES THE PRIVACY COMMISSIONER OF CANADA HANDLE COMPLAINTS?

As an ombudsman, the Commissioner seeks to take a cooperative and conciliatory approach to investigations whenever possible. The Commissioner encourages the resolution of complaints through negotiation and persuasion. Alternate dispute resolution methods such as mediation and conciliation may be used to settle matters at any stage of the investigation process.

Early resolution

Complaints which are identified as having the potential to be resolved quickly are transferred to an Early Resolution Officer.

These complaints include matters where the Office has already made findings on the issue(s) raised by the complaint, where the organization has already dealt with the allegations to the satisfaction of the OPC or where it seems possible that the allegations can be easily addressed.

The OPC helps identify a solution that satisfies all parties without a formal investigation being undertaken when a matter is successfully addressed through this early resolution process. No report of findings will be issued.

Decline to investigate

The Commissioner may decline to accept a complaint for investigation where he or she is of the opinion that:

- the complainant ought to exhaust grievance or review procedures otherwise available;
- the complaint could more appropriately be dealt with, initially or completely, by means of a different procedure provided for under federal or provincial law ; or
- the complaint was not filed within a reasonable time period after the day on which the subject matter of the complaint arose.

When a complaint is declined, the parties to the complaint will be informed of the decision and provided with reasons.

Investigations

Once a complaint has been accepted for investigation (see Declined to Investigate and Intake), an investigator is assigned to the file.

At the outset of an investigation, the Commissioner will notify the organization in writing of the substance of the complaint and will identify the investigator responsible for the case. The organization may submit representations to the Commissioner at any time during the process.

The investigator will contact the organization's designated staff member to indicate how he or she intends to proceed with the investigation and, if possible, which records need to be reviewed and which staff members may be interviewed. The investigator may also indicate whether on-site visits will be needed.

Investigators obtain information directly from individuals familiar with the matter under investigation. These interviews are conducted in private. Investigators may also require access to original documents. Documents given to an investigator are returned within 10 days of a request for their return, but they may be asked for again if the need arises.

Prior to finalizing the investigation, the results are disclosed to the parties involved. They may make additional representations if they see fit. This also gives them the opportunity to resolve the matter before the complaint is finalized.

Although the Commissioner has the power to summon witnesses, administer oaths and compel the production of evidence, these means are only likely to be used if voluntary cooperation is not forthcoming.

The investigator submits the results of the investigation to the Commissioner along with any representations. The Commissioner will consider the case and issue a report to the parties. The Commissioner can request that an organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement report recommendations, or explain why no action has or will be taken.

The report includes the results of the investigation, any settlement reached by the parties, recommendations such as suggested changes in information management practices, what steps the organization has taken or will take to address these recommendations and, if applicable, notice of recourse to the Federal Court.

Findings and Dispositions

A complaint may be disposed of in one of the following ways:

No jurisdiction
Based on the preliminary information gathered, it was determined that PIPEDA did not apply to the organization or activity that was the subject of the complaint. The Commissioner does not issue a report.

Declined to Investigate
The Commissioner declined to commence an investigation in respect of a complaint because he or she was of the view that the complainant ought first to exhaust grievance or review procedures otherwise reasonably available; the complaint could be more appropriately dealt with by means of another procedure provided for under the laws of Canada or of a province; or, the complaint was not

filed within a reasonable period after the day on which the subject matter of the complaint arose, as set out in subsection 12(1) of PIPEDA.

Discontinued
The investigation was discontinued before the allegations were fully investigated. An investigation may be discontinued at the Commissioner's discretion for the reasons set out in subsection 12.2(1) of PIPEDA.

Withdrawn
The complainant voluntarily withdrew the complaint or could no longer be practicably reached. The Commissioner does not issue a report.

Early resolved
The OPC helped negotiate a solution that satisfied all involved parties, without a formal investigation being undertaken. The Commissioner does not issue a report.

Settled
The OPC helped negotiate a solution that satisfied all involved parties during the course of the investigation. The Commissioner does not issue a report.

Not well-founded
The investigation uncovered no, or insufficient evidence to conclude that an organization contravened PIPEDA.

Well-founded and conditionally resolved
The Commissioner determined that an organization contravened a provision of PIPEDA. The organization committed to implementing the recommendations made by the Commissioner and demonstrating their implementation within the timeframe specified.

Well-founded and resolved
The Commissioner determined that an organization contravened a provision of PIPEDA. The organization demonstrated it had taken satisfactory corrective action to remedy the situation, either proactively or in response to recommendations made by the Commissioner, by the time the finding was issued.

Well-founded
The Commissioner determined that an organization contravened a provision of PIPEDA.

Cooperation with other data protection authorities

As a result of amendments to PIPEDA that came into force in 2011, the Office of the Privacy Commissioner of Canada is able to collaborate and share information with persons or bodies in a foreign state that have similar legislated functions and duties or with persons or bodies who have legislated responsibilities relating to conduct that would be a contravention of PIPEDA.

TO LEARN MORE

For more detailed information, please see the following documents on our website:

Organizations' Guide to Complaint Investigations under the *Personal Information Protection and Electronic Documents Act*

Legal information related to the *Personal Information Protection and Electronic Documents Act*

PIPEDA Compliance Framework

APPLICATIONS TO THE FEDERAL COURT

A complainant, or an individual who has been notified that an investigation has been discontinued, may apply to the Federal Court for a hearing in certain cases. As well, the Privacy Commissioner of Canada may apply for a hearing on his or her own or on a complainant's behalf in certain cases. Normally, an application must be made within 45 days of the Commissioner's report or the Commissioner's notification that a complaint has been discontinued.

Applications to the Court must be made in respect of the matter complained of, or of a matter that referred to in the Commissioner's report following an investigation, and must refer to one of the specific provisions identified in section 14 of the Act.

The Federal Court may order an organization to correct practices that do not comply with Sections 5 to 10 of the Act. The Court may also order an organization to publish a notice of any action taken or proposed to correct its practices. The Court can award damages to a complainant, including damages for humiliation.

TO LEARN MORE

For more detailed information, please see the following document on our website:

Fact Sheet - Applications for Court Hearings under PIPEDA

AUDITS OF PERSONAL INFORMATION MANAGEMENT PRACTICES

The Act gives the Privacy Commissioner of Canada the authority to audit an organization's personal information management practices when the Commissioner has reasonable grounds to believe the organization is not fulfilling its obligations under Part 1 of the Act or is not respecting the recommendations of Schedule 1.

WHAT CAN LEAD TO AN AUDIT?

The following are examples of circumstances that may lead the Commissioner to audit the personal information management practices of an organization:

- a group or series of complaints about a particular organization's practice(s)
- information provided by an individual under the whistleblower provision
- an issue receiving media attention.

WHAT TO EXPECT FROM AN AUDIT BY THE COMMISSIONER

In keeping with the Commissioner's ombudsman approach, privacy audits are non-confrontational whenever possible and can be useful for organizations wanting to improve their personal information handling practices.

The Commissioner will inform the organization in writing that an audit will be undertaken. The letter will specify the audit's focus, propose a reasonable time frame, and name the officer authorized to conduct the audit.

Although the Commissioner has the power to summon witnesses, administer oaths and compel organizations to produce evidence, audits are unlikely to be conducted on such a formal basis unless voluntary cooperation is not forthcoming.

The officer will meet with the organization's representative for a preliminary discussion of the intent, purpose and scope of the review.

When the officer requires access to any of the organization's premises, he or she will satisfy security requirements. The officer may interview any person in private on the premises, examine records and obtain copies or extracts of such records. The officer will return any document within 10 days of a request for their return but may ask for them again if the need arises.

Once the audit is finished, the officer will debrief the organization's representative on the findings. The officer will report the audit findings to the Commissioner who will make recommendations. The Commissioner will send the report to the organization and may ask to be kept informed of actions the organization takes to correct problems.

The Commissioner may include the audit report in his or her annual report or may make public the personal information management practices of an organization if the Commissioner considers it to be in the public interest to do so.