Privacy Commissioner of Canada

Your Privacy Responsibilities

Guide for Businesses and Organizations to Canada's *Personal Information Protection and Electronic Documents Act*

About This Guide

This guide helps businesses understand and meet their new obligations under Part 1 of the *Personal Information Protection and Electronic Documents Act*. *

The Act sets out ground rules for the management of personal information in the private sector.

It balances an individual's right to the privacy of personal information with the need of organizations to collect, use or disclose personal information for legitimate business purposes.

The Act establishes the Privacy Commissioner of Canada as the ombudsman for complaints under the new law. The Commissioner seeks whenever possible to solve problems through voluntary compliance, rather than heavy-handed enforcement. The Commissioner investigates complaints, conducts audits, promotes awareness of, and undertakes research about privacy matters. The Commissioner is also the ombudsman for complaints under the *Privacy Act*, which covers the federal public sector.

Part I of the Act comes into force in three phases, beginning January 1, 2001.

For more information, contact:

The Privacy Commissioner of Canada
112 Kent Street
Ottawa ON K1A 1H3

Telephone: 1-613-995-8210
Toll-free: 1-800-282-1376
Fax: 1 613 947-6850
Web site: www.privcom.gc.ca
E-mail: info@privcom.gc.ca

While prepared with care to ensure accuracy and completeness, this guide has no legal status. For the official text of the new law, consult our web site at http://www.privcom.gc.ca or call the Office of the Privacy Commissioner.

Cette publication est également disponible en français.

*This guide deals only with Part I 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, contact the Department of Justice.

Table of Contents

The Act 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 specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

Personal information

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
- 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)

Personal information does not include the name, title, business address or telephone number of an employee of an organization.

Complaints

An individual may complain to the organization in question or to the Privacy Commissioner about any alleged breaches of the law. The Privacy Commissioner may also initiate a complaint.

Application to the Federal Court

After receiving the Commissioner's investigation report, a complainant may apply to the Federal Court for a hearing under certain conditions as set out in Section 14 of the Act. The Privacy Commissioner may also apply to the Court on his own or on the complainant's behalf. The Court may order an organization to change its practices and/or award damages to a complainant, including damages for humiliation suffered.

Audits

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

Whistleblowing

Anyone who believes that any of Sections 5 to 10 of the Act have been or are about to be contravened may notify the Privacy Commissioner, and ask that his or her identity be kept confidential. Once the Privacy Commissioner has given his assurance, he is bound to protect the person's identity.

Offences

It is an offence to:

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

A person is liable to a fine of up to $10,000 on summary conviction or up to $100,000 for an indictable offence.

Definitions

Federal work, undertaking or business

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 some of the specific federal works subject to Part 1 as follows:

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

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 is probably a federal work, undertaking or business.

Commercial activity

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.

Organization

An organization includes an association, a partnership, a person and a trade union.

Consent

Voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. 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.

Disclosure

Making personal information available to others outside the organization.

Use

Refers to the treatment and handling of personal information within an organization.

Is Your Organization Subject to the Act?

The Act affects organizations in three stages:

January 1, 2001

In its first stage, the Act applies to personal information (except personal health information) that is collected, used or disclosed in the course of commercial activities by federal works, undertakings and businesses. This includes, but is not limited to, federally-regulated organizations such as banks, telecommunications and transportation companies.

At this stage the Act also applies to personal data that is collected, used or disclosed by these same organizations about their employees.

In addition, at this stage the Act applies to disclosures of personal information for consideration across provincial or national borders, by organizations such as credit reporting agencies or organizations that lease, sell or exchange mailing lists or other personal information. The information itself must be the subject of the transaction and the consideration is for the information.

January 1, 2002

The Act extends to personal health information for the organizations and activities covered in the first stage. Personal health information is defined as information about an individual's mental or physical health, including information concerning health services provided and information about tests and examinations.

January 1, 2004

The Act extends to the collection, use or disclosure of personal information in the course of any commercial activity within a province. However, the federal government may exempt organizations and/or activities in provinces that have adopted substantially similar privacy legislation.

The Act will also apply to all personal information in all interprovincial and international transactions by all organizations subject to the Act in the course of their commercial activities.

Quebec is the only province that currently has legislation dealing with personal information in the privacy sector. The federal government has stated that this legislation meets the test of "substantially similar" and that organizations and activities subject to the Quebec legislation will be exempted from the federal act for intraprovincial matters.

Other provinces and territories are considering private sector legislation.

A QUICK TEST

Is your organization a federal work, undertaking or business that collects, uses or discloses personal information in the course of a commercial activity?

If YES, you are subject to the Act as of January 1, 2001. It also applies to your employees' personal information as well as your customers'.

If NO:
Do you disclose personal information outside the province for consideration? In other words, is personal information the subject of the transaction?

If YES, that disclosure is subject to the Act beginning January 1, 2001.

What is not Covered by the Act?

- The collection, use or disclosure of personal information 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

Your Responsibilities under the Act

Private sector 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. It lists 10 principles of fair information practices, which form ground rules for the collection, use and disclosure of personal information. These principles give individuals control over how their personal information is handled in the private sector.

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. Care in collecting, using and disclosing personal information is essential to continued consumer confidence and good will.

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 must be read in conjunction with key sections of the Act, including:

Sections 2 to 10 of the Act

Schedule 1 must be read in conjunction with sections 2 to 10 of the Act. It is essential to carefully consider the obligations set out in these sections, along with the ten principles.

Section 2

- Provides definitions including commercial activity, federal work, undertaking or business, personal information, personal health information and organization.
- Specifies that the notes under clauses 4.3 and 4.9 of Schedule 1 **are not** part of the law.

Section 3

Defines the purpose of the Act:

- recognizes individuals' right to privacy of their personal information
- recognizes the need of organizations to collect, use or disclose personal information for legitimate business purposes
- establishes rules for handling personal information

Section 4

Defines the scope of the Act's application:

- covers all organizations that collect, use or disclose personal information in the course of commercial activities
- includes the personal information of an employee of a federal work, undertaking or business **but not** the personal information of other private sector employees

Section 5

- Stipulates that every organization must comply with the obligations of Schedule
- Indicates what is not covered by the Act.
- In the Schedule:
    - "shall" means an obligation.

    - "should" means a recommendation, not an obligation.
- Limits the collection, use and disclosure to purposes that a reasonable person would consider appropriate in the circumstances. The reasonable person's perspective must be taken into account when applying any aspect of Part 1 of the Act.

Section 6

- Establishes that identifying an individual to be accountable for compliance does not mean that the organization is not responsible for its obligations as set out in Schedule 1.

Section 7

- Specifies the circumstances when personal information may be collected, used or disclosed without the individual's consent.

Section 8

- Sets out procedures for individuals to make requests for personal information and corrections to that information.

Section 9

- Explains when access to personal information may be refused.

Section 10

- Defines an organization's obligation to provide personal information in an alternative format (e.g. Braille, large print, or audio tape) to a person with a sensory disability.

Fair Information Principles

- The following section sets out the responsibilities for each of the 10 fair information principles of Schedule 1. It outlines how to fulfil these responsibilities and offers some tips.

The Reasonable Person

Section 5 of the Act limits the collection, use and disclosure for purposes that a "reasonable person" would consider appropriate in the circumstances.

Examples:

- Would a customer renting a movie from a video store consider it reasonable to be required to provide a telephone number? An address? A Social Insurance Number?
- Would a customer paying cash for a product or service consider it reasonable to

be asked for a name, address and phone number?

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 fulfil these responsibilities

- 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 web sites and in publications).
- Analyze 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?
  - 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 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,
  - process access requests, and
  - respond to inquiries and complaints.
- Include a privacy protection clause in contracts to guarantee that the third party provides the same level of protection as your organization does.
- Inform and train staff on privacy policies and procedures.
- Make information available explaining these policies and procedures to clients and customers (e.g. in brochures and on web sites).

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 my privacy protections and rights? (This applies to employees in federally regulated organizations.)
- What are the ongoing activities and new initiatives relating to the protection of personal information at our organization?

When transferring personal information to third parties, 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.

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 fulfil 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

Grandfathering

Personal information that your company has collected during the course of its commercial activities is subject to the Act. Since it has already been collected, you don't need to recollect it. However, in order to continue to use or disclose this information, you now require consent. Some organizations have informed all their customers what they do with their information, to whom it is disclosed and given customers the option to object to these ongoing uses or disclosures.

3. Obtain 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 is identified.

How to fulfil these responsibilities*

- Obtain consent from the individual whose personal information is collected, used or disclosed.
- Communicate in a manner that is clear and can be reasonably understood.
- Record the consent received (e.g. note to file, copy of e-mail, copy of checkoff box).
- Never obtain consent by deceptive means.
- Do not make consent a condition for supplying a product or a service, unless the

information requested is required to fulfil 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 an individual's questions about the purposes of the collection.

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.
- Consent is only meaningful if the individuals understand how their information will be used.
- Consent clauses 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
- Consent can be obtained in person, by phone, by mail, via the Internet etc.
- The form of consent should take into consideration:
  - reasonable expectations of the individual
  - circumstances surrounding the collection
  - sensitivity of the information involved
- Express 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.

* There are some exceptions to the principle of obtaining consent.

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 fulfil 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.

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 fulfil 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 that no longer fulfils its intended purpose.
- Dispose of personal information in a way that prevents improper access. Shredding paper files or deleting electronic records are ideal.
- 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.

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 fulfil 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.
- Update personal information only when necessary to fulfil the specified purposes.
- Keep frequently used information accurate and up to date unless there are clearly set out limits to this requirement.

TIPS

- One way to determine if information needs to be updated is to ask whether the use or disclosure of out of date or incomplete information would harm 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.

How to fulfil 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, anonymizing software)
  - organizational controls (security clearances, limiting access on a "need-to-know" basis, staff training, confidentiality agreements)
- 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 masked 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.

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 fulfil 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.

TIP

- Information about these policies and practices may be made available in person, in writing, by telephone, in publications or on your organization's web site.

9. Give individuals access

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 below).
- An organization should note any disagreement on the file and advise third parties where appropriate.

How to fulfil 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 can 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.
- Give access at minimal or no cost to the individual.
- Notify the individual of the approximate costs before processing the request.
- Give individuals access to their personal information.
- 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.
- There are some exceptions to the principle of providing access.

TIPS

- Keep personal information about individuals in one place to make retrieval easier. Or record where all such information can be found.
- Never disclose personal information unless you are sure of the identity of the requestor and that person’s right of access.
- If you do not store all personal information in one place, keep a record of where the information can be found to make retrieval easier.

10. Provide recourse

Your responsibilities

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

How to fulfil 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 investigation to a person with the skills necessary to conduct it fairly and impartially.
- Give the investigator 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 complaints.

TIPS

- How well your organization handles an individual's complaint may help preserve or restore the individual's confidence in your organization.
- Record all decisions to ensure consistency in applying the Act.

Exceptions to the Consent and Access Principles

There are a number of exceptions to the requirements to obtain consent and provide access set out in the Act.

Exceptions to consent in Section 7

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 before using the information)
- if it is publicly available as specified in regulations
- if the use is clearly in the individual's interest and consent is not available in a timely way
- 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 a government institution that has requested the information, identified its lawful authority, 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 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 believes 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 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
- if required by law.

Exception to access in Section 9

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
- if the organization has disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct the organization to refuse access or not to reveal that the information has been released. The organization must refuse the request and notify the Privacy Commissioner. The organization cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Privacy Commissioner was notified of the refusal.

Organizations **may** refuse access to personal information if the information falls under one of the following:

- solicitor-client privilege
- confidential commercial information *
- disclosure could harm an individual's life or security *
- it 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 must be notified)
- it was generated in the course of a formal dispute resolution process.

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

Role of the Privacy Commissioner of Canada

The Privacy Commissioner of Canada has oversight of both the *Privacy Act* and Part 1 of the *Personal Information Protection and Electronic Documents Act*. These acts protect personal information according to internationally accepted fair information principles and practices.

The Commissioner is an Officer of Parliament, like the Auditor General of Canada or the Chief Electoral Officer. As an Officer 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 his impartiality and open-mindedness in exercising his role as an ombudsman for privacy matters. The Commissioner makes recommendations, not orders. However there is provision to apply to the Federal Court to review a case.

A privacy ombudsman

Nearly two decades of experience investigating complaints under the *Privacy Act* have helped define the Privacy Commissioner's ombudsman role. The Privacy

Commissioner relies on the competence, knowledge and impartiality of his staff to seek whenever possible 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. While the Commissioner protects individual rights, he is also an advocate for the fair information principles that form the foundation of the legislation. The Commissioner's thorough investigations and impartiality protect both individual rights and the organization against unfair accusations.

Specific responsibilities under the Act

The Act makes the Privacy Commissioner responsible for ensuring compliance with the Act and for promoting its purposes.

Compliance roles

The Commissioner has five main ways of ensuring that organizations subject to the Act adhere to its principles:

- investigating complaints
- mediating and conciliating complaints
- auditing personal information management practices
- publicly reporting abuses
- seeking remedies in court.

(See **Complaints to the Privacy Commissioner**, and **Audits of Personal Management Practices**)

Promoting the purposes of the Act

The Commissioner promotes the purposes of the Act in four ways:

- education
- research
- reporting
- consultation and agreements.

Education

The Commissioner's education mandate includes developing and conducting public information programs to encourage and promote understanding of privacy issues.

Research

The Act 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 may also provide grants and contributions for academic or other research on privacy issues.

Reporting

The Commissioner may make public any information about an organization's personal information management practices, if he considers it in the public interest. He reports annually to Parliament on privacy issues including the extent to which provinces have introduced similar legislation.

Consultation and agreements

The Commissioner may enter into agreements with provincial counterparts who have similar powers and duties. These consultations and agreements may cover complaint mechanisms, research, and developing model contracts for protecting personal information. The Commissioner will encourage organizations to develop detailed policies and practices to comply with Part 1 of the Act.

Complaints to the Privacy Commissioner

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. This includes but is not limited to allegations that an organization:

- denies an individual access to personal information
- improperly collects, uses or discloses personal information
- refuses to correct inaccurate or incomplete information
- fails to provide access to personal information in an alternative format to an individual with a sensory disability
- does not use appropriate safeguards to protect personal information.

The Commissioner may initiate a complaint if there are reasonable grounds to believe that an investigation of a matter under Part 1 of the Act is warranted.

Time limits

There is no time limit for filing most types of complaints.

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 handle complaints?

As an ombudsman, the Commissioner seeks to take a cooperative and conciliatory approach to investigations whenever possible. He 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. 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.

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 assigned to the case 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.

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.

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

1. Not well founded

There is no evidence to lead the Commissioner to conclude that the organization violated the Act.

2. Well founded

The investigation revealed that the organization failed to respect a provision of the Act and the complaint was not resolved.

3. Resolved

The investigation supports the complaint, but the organization agrees to take corrective action to remedy the situation. For example, the organization agrees to release personal information previously denied.

The complaint may also be resolved if it appears to be the result of miscommunication or misunderstanding. For example, an organization misunderstood the request and now agrees to release the personal information sought by the complainant.

The complaint is also resolved if the complainant is satisfied with the Commissioner's efforts and the results.

The Commissioner is not required to issue an investigation report if:

- the complainant has not pursued alternate redress mechanisms that are reasonably available;
- the case could be more appropriately dealt with through other legislation;
- too much time has passed since the matter that prompted the complaint and reporting would serve no useful purpose; or,
- the complaint is trivial, frivolous or vexatious, or is made in bad faith.

Public disclosure

The Privacy Commissioner may make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so.

Applications to Federal Court

A complainant may apply to the Federal Court for a hearing. The Privacy Commissioner may apply on his own or on a complainant's behalf. Normally, an application must be made within 45 days of the Commissioner's report.

What Matters Can Be Heard

The Court will consider applications arising from the complaint or any matter referred to in the Commissioner's report and that is referred to in one of the following

Under Schedule 1

4.1.3 Whether an organization has properly exercised its responsibility for the personal information in its possession including information transferred to a third party.

4.2 Whether an organization has properly identified and documented the purposes for which personal information is being collected, used or disclosed, at or before the time of collection.

4.3.3 Whether an organization has refused to provide a service to an individual because the individual would not consent to the collection, use or disclosure of more information than necessary for the specified purpose.

4.4 Whether an organization has collected more information than necessary for the purposes or whether it was collected by fair and lawful means.

4.6 Whether the information is accurate, up-to-date and complete as necessary.

4.7 Whether an organization has taken the necessary steps to safeguard the information.

4.8 Whether an organization has made specific information about its personal information management policies readily available to individuals.

Under Schedule 1 as modified by Sections 5 to 10 of the Act

4.3 Whether personal information has been collected, used or disclosed without the knowledge or consent of the individual, except where permitted or required.

4.5 Whether an organization has used or disclosed personal information for purposes other than those for which it was collected, without the consent of the individual and in circumstances not authorized by the Act. As well, whether an organization has retained the information long enough for a complainant to exhaust his remedies under the Act.

4.9 Whether an individual was wrongly denied access to information about himself except where permitted or required.

Sections of the Act

5(3) Whether the information was collected, used or disclosed only for purposes that a reasonable person would consider appropriate.

8(6) Whether an individual has been charged too much for access to information or was not notified in advance of the cost.

8(7) Whether an organization has informed the individual in writing of a refusal to give access, has given the reasons for the refusal and set out the appropriate recourse available.

10 Whether an organization has failed to grant access in an alternative format to an individual with a sensory disability.

Remedies available through Federal Court

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. There is no ceiling on monetary damages that the Court may award.

Audits of Personal Information Management Practices

The Act gives the Privacy Commissioner the authority to audit an organization's personal information management practices when he 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 Privacy 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 timeframe, and name the officer delegated 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 annual report or he may make public the personal information management practices of an organization if he considers it to be in the public interest to do so.

Privacy Questionnaire

The following are some common sense questions you can use to help your organization implement the Personal Information Protection and Electronic Documents Act. The questionnaire may be used along with the description of the Act in this guide.

If you are unsure about whether or when the Act applies to your organization, please refer to the section *Is your organization subject to the Act* of this guide.

Not all of the following questions will apply to all organizations, as the Act applies to a wide variety and size of organizations. Consider each question along with your organization's current practices. Answering "no" indicates areas that need to be addressed or improved.

Personal information holdings

- Do you know what personal information is?
- Do you collect, use or disclose personal information in your day-to-day commercial activities?
- Do you have an inventory of your personal information holdings?
- Do you know where personal information is held (physical locations and files)?
- Do you know in what format(s) the personal information is kept electronic, paper, etc.)?
- Do you know who has access to personal information in and outside your organization?

Accountability of organization and staff

- Have you named a privacy officer who is responsible for your organization's overall compliance with the Act?
- Is this responsibility shared with more than one person?
- If these responsibilities are shared, have they been clearly identified?
- Can your staff respond to internal and external privacy questions on behalf of the organization, or do they know who should respond?
- Does your staff know who receives and responds to:
  - requests for personal information?
  - requests for correction?
  - complaints from the public?
- Do your customers know whom to contact:
  - for general inquiries regarding their personal information?
  - to request their personal information?
  - to request corrections to their personal information?
  - for complaints?

- Is your privacy officer able to explain to the public the steps and procedures for requesting personal information and filing complaints?
- Has your staff been trained on the Act?
- Will there be ongoing training?
- Is your staff able to explain the purposes for the collection, use and disclosure of personal information to customers in easy to understand terms?
- Is your staff able to explain to customers when and how they may withdraw consent and what the consequences, if any, there are of such a withdrawal?
- Will you inform your employees of new privacy issues raised by technological changes, internal reviews, public complaints and decisions of the courts?

Information for customers and employees

- Do you have documents that explain your personal information practices and procedures to your customers?
- Does this information include how to:
  - obtain personal information?
  - correct personal information?
  - make an inquiry or complaint?
- Does this information describe personal information that is:
  - held by the organization and how it is used?
  - disclosed to subsidiaries and other third parties?
- Do you have a privacy policy for your web site?
- Is your privacy policy prominent and easy to find? Is it easily understandable?
- Do your application forms, questionnaires, survey forms, pamphlets and brochures clearly state the purposes for the collection, use or disclosure of personal information?
- Have you reviewed all your public information material to ensure that any sections concerning personal information are clear and understandable?
- Have you ensured that the public can obtain this information easily and without cost?
- Is this information reviewed regularly to ensure that it is accurate, complete and up to date?
- Does this information include the current name or title of the person who is responsible for overseeing compliance with the Act?

Limiting collection, use, disclosure and retention to identified purposes

- Have you identified the purposes for collecting personal information?
- Are these purposes identified at or before the time the information is collected?
- Do you collect only the personal information needed for identified purposes?
- Do you document the purposes for which personal information is collected?
- If you gather and combine personal information from more than one source, do you ensure that the original purposes have not changed?
- Have you developed a timetable for retaining and disposing of personal information?
- When you no longer require personal information for the identified purposes or it is no longer required by law, do you destroy, erase or make it anonymous?

Consent

- Does your staff know that an individual’s consent must be obtained before or at the time they collect personal information?
- Does your staff know they must obtain an individual’s consent before any new use or new disclosure of the information?
- Do you use express consent whenever possible, and in all cases where the information is sensitive or the individual would reasonably expect it?
- Is your consent statement worded clearly, so that an individual can understand the purpose of the collection, use or disclosure?
- Do you make it clear to customers that they need not provide personal information that is not essential to the purpose of the collection, use or disclosure?

Third party transfers

- Do you use contracts to ensure the protection of personal information transferred to a third party for processing?
- Does the contract limit the third party’s use of information to purposes necessary to fulfil the contract?
- Does the contract require the third party to refer any requests for access or complaints about the information transferred to you?
- Does the contract specify how and when a third party is to dispose of or return any personal information it receives?

Ensuring accuracy

- Is personal information sufficiently accurate, complete and up to date to minimize the possibility that your organization might use inappropriate information?
- Does your organization document when and how personal information is updated, to ensure its accuracy?
- Do you ensure that personal information received from a third party is accurate and complete?

Safeguards

- Have you reviewed your physical, technological and organizational security measures?
- Do they prevent improper access, modification, collection, use, disclosure and/or disposal of personal information?
- Is personal information protected by security safeguards that are appropriate to the:
    - sensitivity of the information?
    - scale of distribution?
    - format of the information?
    - method of storage?
- Have you developed a "need-to-know" test to limit access to personal

information to what is necessary to perform assigned functions?
- Has your staff been trained about security practices to protect personal information? For example, is staff aware that personal information should not be left displayed on their computer screens or desktops in their absence?
- Is your staff aware that they should properly identify individuals and establish their right to access the personal information before disclosing it?
- Do you have rules about who is permitted to add, change or delete personal information?
- Is there a records management system that assigns user accounts, access rights and security authorizations?
- Do you ensure that no unauthorized parties may dispose of, obtain access to, modify or destroy personal information?

Requests for access to personal information

- Is your staff aware of the time limits the law allows to respond to access requests?
- Can you retrieve personal information to respond to individual access requests with a minimal disruption to operations?
- Do your information systems facilitate the retrieval and accurate reporting of an individual's personal information, including disclosures to third party organizations?
- Do you provide personal information to the individual at minimal or no cost?
- Do you advise requesters of costs, if any, before personal information is retrieved?
- Do you record an individual's response to being notified of the cost of retrieving personal information?
- Do you provide personal information in a form that is generally understandable? (For example, do you explain abbreviations?)
- Does your organization have procedures for responding to requests for personal information in an alternate format (such as Braille or audio tapes)?

Handling complaints

- Can an individual easily find out how to file a complaint with you?
- Do you deal with complaints in a timely fashion?
- Do you investigate all complaints received?
- Are your customer assistance and other front-line staff able to distinguish a complaint under the law from a general inquiry? If unsure, do they discuss this with the individual?
- Do you advise individuals about all available avenues of complaints, including the Privacy Commissioner of Canada?
- Are staff responses to public inquiries, requests and complaints reviewed to ensure they are handled fairly, accurately and quickly?
- When a complaint is found to be justified, do you take appropriate corrective measures, such as amending your policies and advising staff of the outcome?