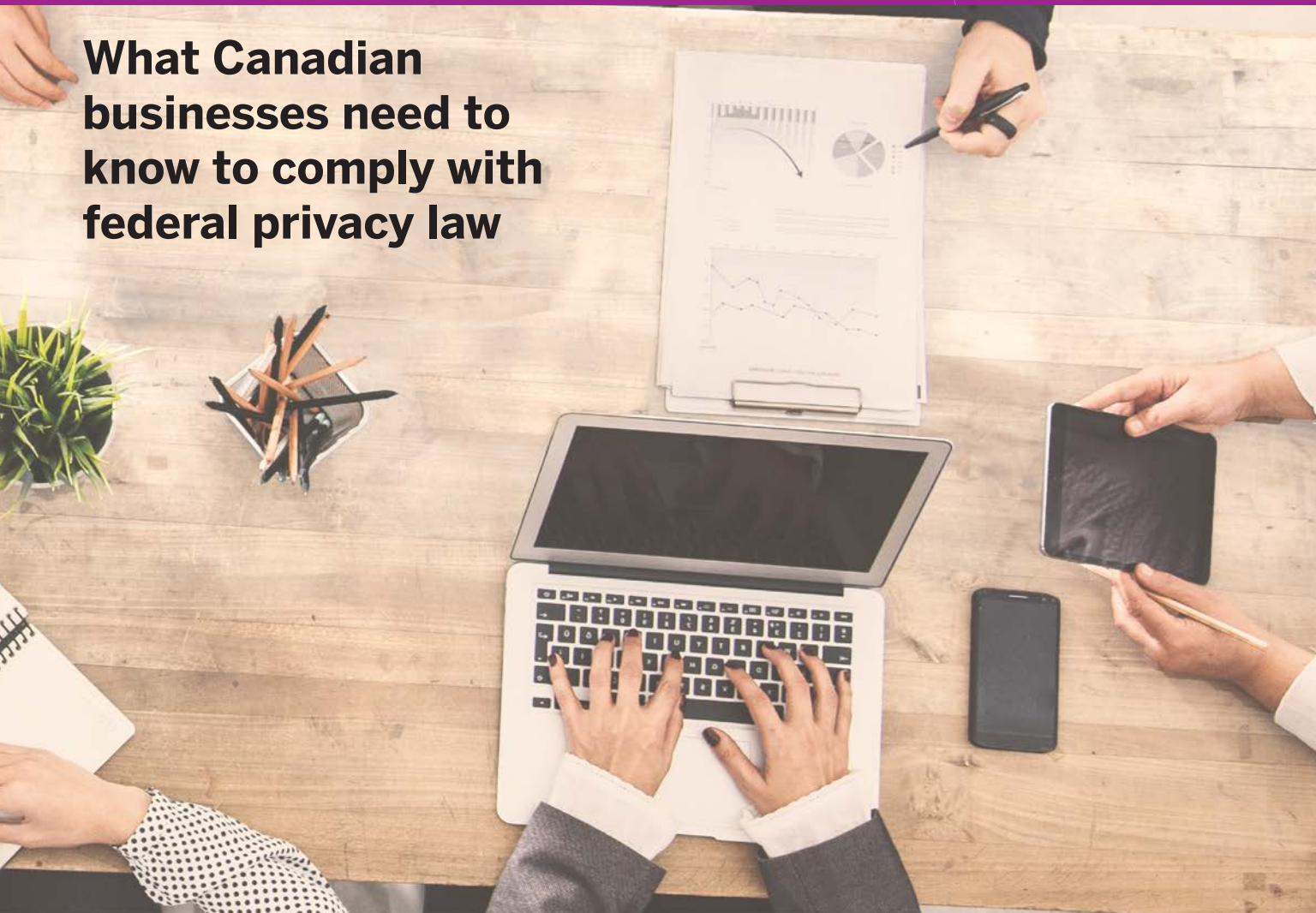
Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Privacy Guide for Businesses

What Canadian businesses need to know to comply with federal privacy law



For more information, contact:

Office of the Privacy Commissioner of Canada
30 Victoria Street, 8th floor
Gatineau, QC
K1A 1H3

Telephone: (819) 994-5444
Toll-free: 1-800-282-1376
TTY: (819) 994-6591

For more information visit: priv.gc.ca/business
Follow us on Twitter: @privacyprivee

Cat. No. IP54-94/2019E
ISBN 978-0-660-32104-2

Updated September 2020

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.

Table of contents

Overview

Canadians are increasingly concerned about their privacy. More and more, they are choosing to do business with organizations that are sensitive to those concerns and can demonstrate they will handle personal information with care.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada's federal private-sector privacy law. It sets out the ground rules for how businesses must handle personal information in the course of commercial activities.

The Office of the Privacy Commissioner of Canada (OPC) has prepared this guide to help organizations understand and meet their obligations under PIPEDA.

Role of the Office of the Privacy Commissioner of Canada

The OPC's mission is to protect and promote privacy rights. As an Agent of Parliament, the Privacy Commissioner reports directly to the House of Commons and the Senate of Canada. This independence helps ensure the Commissioner is impartial in exercising the role of ombudsman for privacy issues.

The OPC oversees compliance with PIPEDA by conducting independent and impartial investigations and/or audits into the personal information handling practices of businesses.

The OPC also seeks to ensure that organizations comply with their privacy obligations by providing them with information and guidance. The Office also undertakes engagement activities, which include outreach and advisory services.

PIPEDA in brief

There are a number of requirements to comply with the law. Organizations covered by PIPEDA must generally obtain an individual's consent when they collect, use or disclose that individual's personal information. People have the right to access their personal information held by an organization. They also have the right to challenge its accuracy.

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, it must obtain consent again. Personal information must be protected by appropriate safeguards.

How the act applies

PIPEDA applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity.

The law defines a commercial activity 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 fundraising lists.

Provincial privacy laws

Alberta, British Columbia and Quebec have their own private-sector privacy laws that have been deemed substantially similar to PIPEDA. Organizations subject to a substantially similar provincial privacy law are generally exempt from PIPEDA with respect to the collection, use or disclosure of personal information that occurs within that province.

Ontario, New Brunswick, Nova Scotia and Newfoundland and Labrador have also adopted substantially similar legislation regarding the collection, use and disclosure of personal health information.

Information that crosses borders

All businesses that operate in Canada and handle personal information that crosses provincial or national borders in the course of commercial activities are subject to PIPEDA, regardless of the province or territory in which they are based (including provinces with substantially similar legislation).

Federally regulated organizations

Federally regulated organizations that conduct business in Canada are always subject to PIPEDA. The Act also applies to their employees' personal information.

These organizations include:

- airports, aircraft and airlines;
- banks and authorized foreign banks;
- inter-provincial or international transportation companies;
- telecommunications companies;
- offshore drilling operations; and
- radio and television broadcasters.

Note: Organizations in the Northwest Territories, Yukon and Nunavut are considered federally regulated, and are therefore also covered by PIPEDA.

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 handled by federal government organizations listed under the Privacy Act;
- provincial or territorial governments and their agents;
- business contact information such as an employee's name, title, business address, telephone number or email address that is collected, used or disclosed solely for the purpose of communicating with that person in relation to their employment or profession;
- an individual's collection, use or disclosure of personal information strictly for personal purposes (e.g. personal greeting card list); and
- an organization's collection, use or disclosure of personal information solely for journalistic, artistic or literary purposes.

Unless they are engaging in commercial activities that are not central to their mandate and involve personal information, PIPEDA does not generally apply to:

- not-for-profit and charity groups; or
- political parties and associations.

Municipalities, universities, schools, and hospitals are generally covered by provincial laws. PIPEDA may apply in certain situations.

Your responsibilities under PIPEDA

Businesses must follow the 10 fair information principles to protect personal information, which are set out in Schedule 1 of PIPEDA.

By following these principles, you will contribute to building trust in your business and in the digital economy.

The principles 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

Fair information principles

PIPEDA's 10 fair information principles form the ground rules for the collection, use and disclosure of personal information, as well as for providing access to personal information. They give individuals control over how their personal information is handled in the private sector.

In addition to these principles, PIPEDA states that any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider appropriate in the circumstances.

The OPC has determined that the following purposes would generally be considered inappropriate by a reasonable person (i.e., no-go zones):

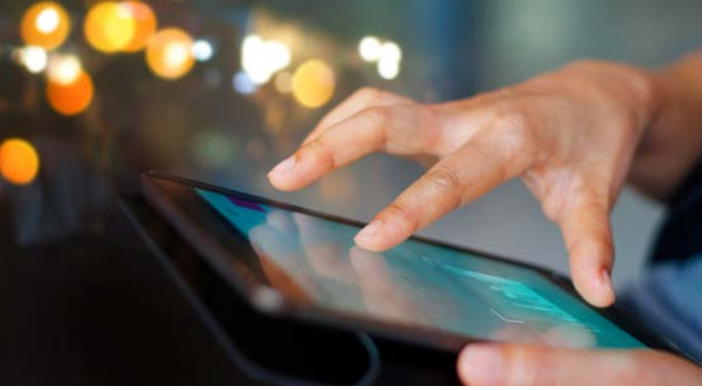
- collecting, using or disclosing personal information in ways that are otherwise unlawful;
- profiling or categorizing individuals in a way that leads to unfair, unethical or discriminatory treatment contrary to human rights law;
- collecting, using or disclosing personal information for purposes that are known or likely to cause significant harm to the individual;
- publishing personal information with the intent of charging people for its removal;
- requiring passwords to social media accounts for the purpose of employee screening; and
- conducting surveillance on an individual using their own device's audio or video functions.

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

1 Be accountable

Your responsibilities

- Comply with all 10 fair information principles.
- Appoint someone to be responsible for your organization's PIPEDA compliance.
- Protect all personal information held by your organization, including any personal information you transfer to a third party for processing.
- Develop and implement personal information policies and practices.



How to fulfill these responsibilities

Develop a privacy management program

- This program should be designed, at a minimum, to comply with the law, including the 10 fair information principles.
- It should identify your organization's designated privacy official, and communicate that person's name or title internally and externally (e.g. on your website or in publications).
- Your designated privacy official should have the support of senior management and the authority to intervene on privacy issues.
- Conduct a privacy impact assessment and threat analysis of your organization's personal information handling practices, including ongoing activities, new initiatives, and new technologies.
- Start by using the following checklist:
  - » 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?
  - » Who do we share it with?
  - » When is it disposed of?
- Develop, document and implement policies and procedures to protect personal information:
  - » Define the purposes of collection.
  - » Obtain valid and meaningful consent.
  - » Limit collection, use and disclosure.
  - » Ensure information is correct, complete and current.
  - » Ensure security measures are adequate to protect information.
  - » Develop or update a retention and destruction timetable.
  - » Develop and implement policies and procedures to respond to complaints, inquiries and requests to access personal information.
  - » Develop, document and implement breach and incident-management protocols.
  - » Document and implement risk assessments.
  - » Develop, document and implement appropriate practices to be used by third-party service-providers.
  - » Develop, document and deliver appropriate privacy training for employees.
- Regularly review your privacy management program and address any shortcomings.
- Be prepared to demonstrate that you have specific policies and procedures in place to protect personal information; that you provide adequate privacy training to your employees; and that you have appointed someone to be responsible for privacy governance.
- Make your privacy policies and procedures readily available to customers and employees (e.g., in brochures and on websites).

Tips

Train all staff so they can answer the following questions:

- How do I respond to public inquiries regarding our organization's privacy policies?
- What is valid and meaningful consent? When and how is it obtained?
- How do I recognize and process requests for access to personal information?
- To whom should I refer privacy-related complaints?
- What are my organization's current or new initiatives relating to the protection of personal information?

When transferring personal information to third parties for processing outside Canada:

- assess risks that could adversely impact the protection of personal information when it is transferred to third-party service providers operating outside of Canada;
- ensure through contractual or other means that the third party provides a level of protection of the personal information comparable to that required in PIPEDA;
- limit the third party's use of the personal information to the purposes specified to fulfill the contract; and
- be transparent about your practices, including by advising customers their information may be sent to another jurisdiction for processing, and that while in another jurisdiction it may be accessed by the courts, law enforcement and national security authorities.

Related links

- PIPEDA Fair Information Principle 1 – Accountability
- Getting Accountability Right with a Privacy Management Program
- Interpretation bulletin: Accountability

2 Identify the purpose

Your responsibilities

- Identify and document your purposes for collecting personal information. This will help you determine which specific personal information to collect to fulfill those purposes.
- Tell your customers why your organization needs their personal information before or at the time of collection. Depending on how the information is collected, this can be done orally or in writing.
- Obtain their consent again should you identify a new purpose.

How to fulfill these responsibilities

- Review your personal information holdings to ensure they are all required for a specific purpose.
- When requesting personal information from a customer, explain these purposes to them, either verbally or in writing.
- Keep a record of all identified purposes and consents you have obtained.
- Ensure that the purposes are limited to what a reasonable person would consider appropriate under the circumstances.

Tips

Define your purposes for collecting personal information as clearly and narrowly as possible so people understand how their information will be used or disclosed. Examples of specific purposes include:

- opening an account;
- verifying an individual's creditworthiness;
- providing benefits to employees;
- processing a magazine subscription;
- sending out association membership information;
- guaranteeing a travel reservation;
- identifying customer preferences; and
- establishing customer eligibility for special offers or discounts.

Avoid overly broad purposes.

Related link

- PIPEDA Fair Information Principle 2 – Identifying Purposes

3 Obtain valid, informed consent

Your responsibilities

- Meaningful consent is an essential element of PIPEDA. Organizations are generally required to obtain meaningful consent for the collection, use and disclosure of personal information.
- To make consent meaningful, people must understand what they are consenting to. It is only considered valid if it is reasonable to expect that your customers will understand the nature, purpose and consequences of the collection, use or disclosure of their personal information.
- Consent can only be required for collections, uses or disclosures that are necessary to fulfil an explicitly specified and legitimate purpose. For non-integral collections, uses and disclosures, individuals must be given a choice.
- The form of consent must take into account the sensitivity of the personal information. The way you seek consent will depend on the circumstances and type of information you are collecting.
- Individuals can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and you must inform individuals of the implications of withdrawal.

How to fulfill these responsibilities

- Make privacy information readily available in complete form, while giving emphasis or bringing attention to four key elements:
  - what personal information is being collected, with sufficient precision for individuals to meaningfully understand what they are consenting to;
  - with which parties personal information is being shared;

  - » for what purposes personal information is being collected, used or disclosed, in sufficient detail for individuals to meaningfully understand what they are consenting to; and
  - » what are the risks of harm and other consequences.
- Provide information in manageable and easily accessible ways.
- Make available to individuals a clear and easily accessible choice for any collection, use or disclosure that is not necessary to provide the product or service.
- Consider the perspective of your consumers, to ensure consent processes are user-friendly and generally understandable.
- Obtain consent when making significant changes to privacy practices, including use of data for new purposes or disclosures to new third parties.
- Only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate under the circumstances.
- Allow individuals to withdraw consent (subject to legal or contractual restrictions).
- Determine the appropriate form of consent: obtain express (explicit) consent for collections, uses or disclosures which generally: (i) involve sensitive information; (ii) are outside the reasonable expectations of the individual; and/or (iii) create a meaningful residual risk of significant harm.
- Consent and children: obtain consent from a parent or guardian for any individual unable to provide meaningful consent themselves (the OPC takes the position that, in all but exceptional circumstances, this includes anyone under the age of 13), and ensure that the consent process for youth able to provide consent themselves reasonably considers their level of maturity.
- Whether implied or express, consent does not waive an organization's other responsibilities under PIPEDA, such as being accountable, implementing safeguards, and having a reasonable purpose for processing personal information.

Form of consent

It is important for organizations to consider the appropriate form of consent to use (express or implied) for any collection, use or disclosure of personal information for which consent is required. While consent should generally be express, it can be implied in strictly defined circumstances. Organizations need to take into account the sensitivity of the information and the reasonable expectations of the individual, both of which will depend on context.

Organizations must generally obtain *express* consent when:

- the information being collected, used or disclosed is sensitive;
- the collection, use or disclosure is outside of the reasonable expectations of the individual; and/or,
- the collection, use or disclosure creates a meaningful residual risk of significant harm.

Tips

The following tips can help make your consent process more meaningful:

- Allow individuals to control the amount of detail they wish to receive, and when.
- Design or adopt innovative and creative ways of obtaining consent, which are just-in-time, specific to the context, and suitable to the type of interface.
- Periodically remind individuals about the consent choices they have made, and those available to them.
- Periodically audit privacy communications to ensure they accurately reflect current personal information management practices.
- Stand ready to demonstrate compliance – in particular, that the consent process is understandable from the perspective of the user.
- In designing consent processes, consider:
  - consulting with users and seeking their input;
  - pilot testing or using focus groups to evaluate the understandability of documents;
  - involving user interaction / user experience (UI/UX) designers;
  - consulting with privacy experts and/or regulators; and
  - following established best practices or standards.

Related links

- PIPEDA Fair Information Principle 3 – Consent (includes exceptions to the consent principle)
- Guidelines for obtaining meaningful consent
- Ten tips for a better online privacy policy and improved privacy practice transparency

4 Limit collection

Your responsibilities

- Collect only the personal information your organization needs to fulfill a legitimate identified purpose.
- Be honest about the reasons you are collecting personal information.
- Collect personal information by fair and lawful means. This requirement is intended to prevent organizations from collecting information by misleading or deceiving about the purpose.

How to fulfill these responsibilities

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

Tips

- By reducing the amount of information gathered, you can lower the cost of collecting, storing, retaining and ultimately archiving or disposing of data.
- Collecting less information also reduces the risk and/or impact of loss or inappropriate access, use or disclosure.

Related links

- PIPEDA Fair Information Principle 4 – Limiting Collection
- Collection of driver's licence numbers under private sector privacy legislation – A guide for retailers
- 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

- Unless someone consents otherwise—or unless doing so is required by law—your organization may use or disclose personal information only for the identified purposes for which it was collected. Keep personal information only as long as it is needed to serve those purposes.
- Know what personal information you have, where it is, and what you are doing with it.
- Obtain fresh consent if you intend to use or disclose personal information for a new purpose.
- Collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.
- 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 may be useful in the event an individual seeks access to the information in order to pursue redress.
- Destroy, erase or anonymize any personal information that your organization no longer needs.

How to fulfill these responsibilities

- Document any new purpose for the use of personal information.
- Limit and monitor employee access to personal information, and take appropriate action when information is accessed without authorization.
- Institute maximum and minimum retention periods that take into account any legal requirements or restrictions as well as appeal mechanisms.
- Dispose of personal information that does not have a specific purpose or no longer fulfills its intended purpose. Dispose of information in a way that prevents a privacy breach, such as by securely shredding paper files or effectively deleting electronic records. If information is to be retained purely for statistical purposes, employ effective techniques that would render it anonymous.
- Ensure all personal information is fully deleted before disposing of electronic devices such as computers, photocopiers and cellphones.
- Ensure your employees receive appropriate training on their roles and responsibilities in protecting personal information.

Tips

- Use effective processes for destroying, erasing or anonymizing personal information.
- Develop guidelines and implement procedures on the retention of personal information.
- Conduct regular reviews to determine whether information is still required.
- Establish a retention schedule to make this easier.

Related links

- PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention
- PIPEDA and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*
- Personal information retention and disposal: principles and best practices

6 Be accurate

Your responsibility

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

How to fulfill this responsibility

- Keep personal information as accurate, complete and up to date as necessary, taking into account its use and the interests of the individual.
- Establish policies that govern what types of information need to be updated.

Tips

One way to determine whether information needs to be updated is to ask yourself whether using or disclosing out-of-date or incomplete information could potentially have an adverse impact on the individual.

Apply the following checklist for accuracy:

- List the specific items of personal information you need to provide a service.
- List where all related personal information can be found.
- Record the date when the personal information was obtained or updated.
- Record the steps taken to verify the accuracy, completeness and timeliness of the information. This may require reviewing your records or communicating with your customer.

Related link

- PIPEDA Fair Information Principle 6 – Accuracy

7 Use appropriate safeguards

Your responsibilities

- Protect personal information in a way that is appropriate to how sensitive it is.
- Protect all personal information (regardless of how it is stored) against loss, theft, or any unauthorized access, disclosure, copying, use or modification.

Note: PIPEDA does not specify particular security safeguards that must be used. Your organization must continually ensure it adequately protects the personal information in its care as technologies evolve and as new risks emerge.

How to fulfill these responsibilities

- Develop and implement a security policy to protect personal information.
- Use appropriate security safeguards to provide necessary protection. These can include:
  - » physical measures (e.g., locked filing cabinets, restricting access to offices, and alarm systems);
  - » up-to-date technological tools (e.g., passwords, encryption, firewalls and security patches); and
  - » organizational controls (e.g., security clearances, limiting access, staff training and agreements).

- Consider the following factors when selecting the right safeguard:
  - » the sensitivity of the information and the risk of harm to the individual. For instance, health and financial information would be considered highly sensitive;
  - » the amount of information;
  - » the extent of distribution;
  - » the format of the information (e.g., electronic or paper);
  - » the type of storage; and
  - » the types and levels of potential risk your organization faces.
- Review security safeguards regularly to ensure they are up to date, and that you have addressed any known vulnerabilities through regular security audits and/or testing.
- Make your employees aware of the importance of maintaining the security and confidentiality of personal information, and hold regular staff training on security safeguards.

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 files that contain sensitive information in a secure area or on a secure computer system, and limit employee access to a "need-to-know" basis.

Related links

- PIPEDA Fair Information Principle 7 – Safeguards
- Safeguarding personal information
- Securing Personal Information: A Self-Assessment Tool for Organizations
- Interpretation bulletin: Safeguards
- 10 tips for addressing employee snooping
- What you need to know about mandatory reporting of breaches of security safeguards
- Preventing and responding to a privacy breach

Note: For information on breaches, see the section on this topic.

8 Be open

Your organization's detailed personal information management practices must be clear and easy to understand. They must be readily available.

Consumers find privacy policies are difficult to understand, yet they feel compelled to give their consent in order to obtain the goods and services they want.

Individuals should not be expected to decipher complex legal language in order to make informed decisions on whether or not to provide consent. (See Principle 3 on consent for details).

Your responsibilities

- Inform your customers and employees that you have policies and practices for managing personal information.
- Make these policies and practices easily understandable and easily available.

How to fulfill these responsibilities

- Comply with guidelines on obtaining meaningful consent.
- Ensure your front-line staff is familiar with your organization's procedures for responding to people's inquiries about their personal information.
- Provide, in easy-to-understand terms:
  - » the name or title and contact information of the person who is accountable for your organization's privacy policies and practices;
  - » the name or title and contact information of the person to whom access requests should be sent;
  - » how an individual can gain access to their personal information;
  - » how an individual can complain to your organization;
  - » any documents that explain your organization's policies, standards or codes; and
  - » a description of what personal information you disclose to other organizations, including your subsidiaries and any third parties, and why.

Tips

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

Related links

- PIPEDA Fair Information Principle 8 – Openness
- 10 tips for a better online privacy policy and improved privacy practice transparency
- Guidelines for obtaining meaningful consent

9 Give individuals access

Generally speaking, individuals have a right to access the personal information that an organization holds about them. They also have the right to challenge the accuracy and completeness of the information, and have that information amended as appropriate.

Your responsibilities

- When asked, advise people about the personal information about them your organization holds.
- Explain where the information was obtained.
- Explain how that information is or has been used and to whom it has been disclosed.
- Give people access to their information at minimal or no cost, or explain your reasons for not providing access. Providing access can take different forms. For example, you may provide a written or electronic copy of the information, or allow the individual to view the information or listen to a recording of the information.
- Correct or amend personal information in cases where accuracy and completeness is deficient.
- Note any disputes on the file and advise third parties where appropriate.

How to fulfill these responsibilities

- Help people prepare their request for access to personal information. (For example, your organization may ask the requestor to supply enough information to enable you to locate personal information and determine how it has been used or disclosed.)
- Respond to the request as quickly as possible, and no later than 30 days after receiving it.
- The normal 30-day response time limit for access requests may be extended for a maximum of 30 additional days, if:
  - » responding to the request within the original 30 days would unreasonably interfere with the activities of your organization;
  - » your organization needs additional time to conduct consultations; or
  - » your organization needs additional time to convert personal information to an alternate format.
- If your organization extends this response time, it must notify the person making the request within 30 days of receiving the request, and advise them of their right to complain to the OPC.
- Provide access at minimal or no cost to the individual, and notify the requestor of the approximate cost before processing the request. Confirm that the individual still wants to proceed with the request.
- Make sure the requested information is understandable. Explain acronyms, abbreviations and codes.

- If you make amendments, send the revised information to any third parties that have access to the information in cases where doing so is appropriate.
- If you refuse to grant access to personal information, explain in writing the reasons and inform the requestor of any recourse available to them. Recourse includes the option to complain to the OPC.
- If your organization holds no personal information on the requestor, tell them so.

Tips

- Keep a record of where personal information can be found.
- Conduct a thorough search for personal information. This includes both physical and electronic searches.
- Never disclose personal information unless you are certain of the identity of the requestor and that person's right of access.
- Record the date you received the request for the information.
- Ensure your staff members know how to handle an access request.
- The legal standard to be met for withholding information as "confidential commercial information" is high. Be ready to justify such a claim before refusing access.

Related links

- PIPEDA Fair Information Principle 9 – Individual Access
- Responding to access to information requests under PIPEDA

10 Challenging compliance

An individual must be able to challenge your organization's compliance with the fair information principles. They should address their challenge to the person in your organization who is accountable for compliance with PIPEDA.

Your responsibilities

- Provide recourse by developing simple complaint handling and investigation procedures.
- Tell complainants about their avenues of recourse. These include your organization's own complaint procedures, along with those related to industry associations, regulatory bodies and the OPC.
- Investigate all complaints you receive.
- Improve any information-handling practices and policies that are found to be problematic.

How to fulfill these responsibilities

- Record the date on which you receive a complaint, and its nature.
- Acknowledge receipt of the complaint promptly, and seek clarification if needed.
- Assign the matter to a person with the skills necessary to review it fairly and impartially. Provide that person with access to all relevant records, employees or others who handled the personal information or access request.
- Notify individuals of the outcome of complaint reviews clearly and promptly, and inform them of any steps taken.
- Correct any inaccurate personal information or modify policies and procedures based on the outcome of the complaint. Ensure employees are aware of any changes to policies and procedures.

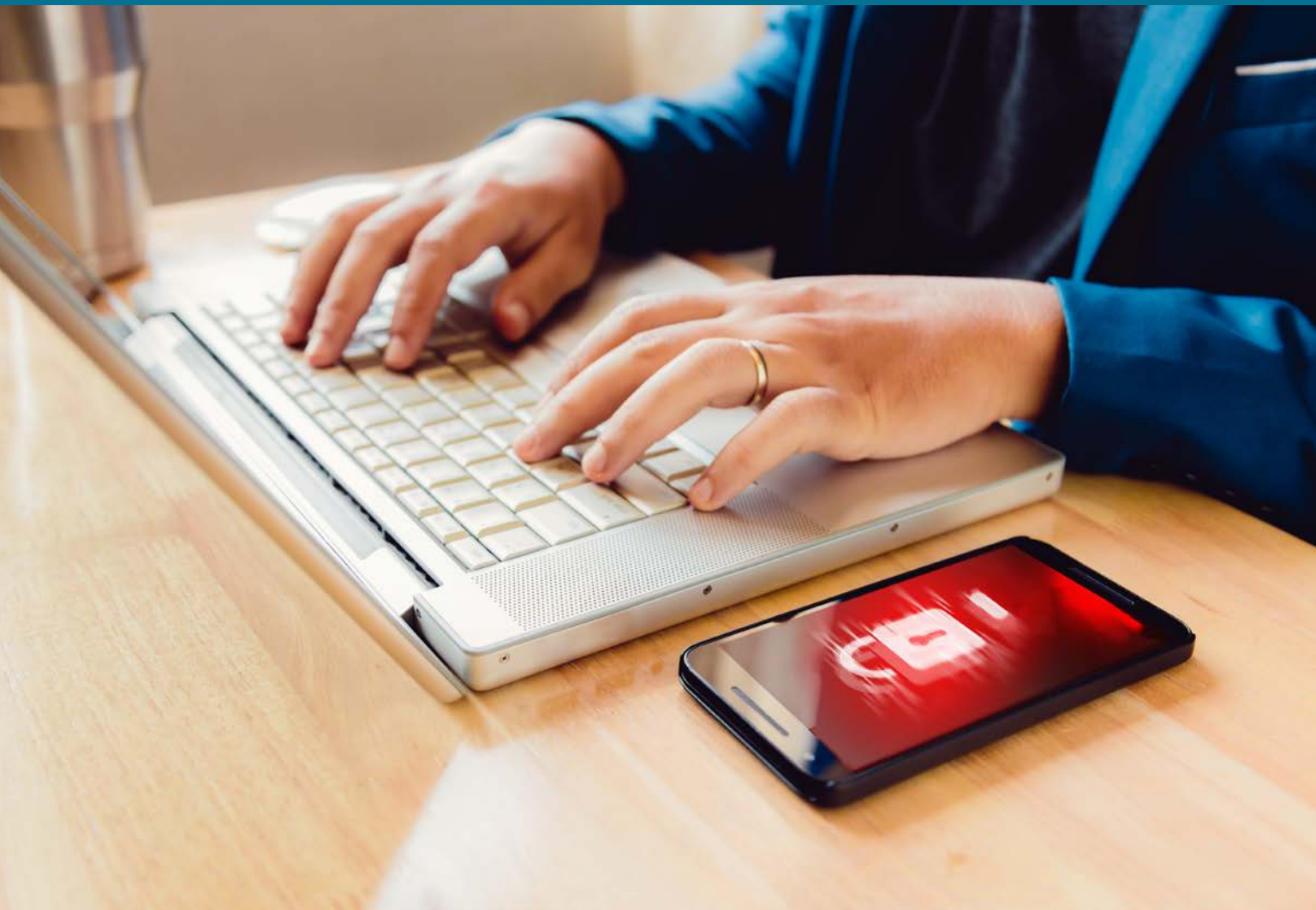
Tips

- Handling a complaint fairly may help to preserve or restore your customer's confidence and trust in your organization.
- Ensure staff members are aware of the policies and procedures for complaints, and know who is responsible for handling complaints.
- Record all your decisions to ensure consistency.

Related links

- PIPEDA Fair Information Principle 10 – Challenging Compliance
- Getting Accountability Right with a Privacy Management Program
- Ten tips for avoiding complaints to the OPC

Dealing with a breach



A breach of security safeguards occurs when there is a loss, unauthorized access to, use or disclosure of personal information. PIPEDA includes mandatory breach reporting requirements.

Organizations must:

- report to the OPC any breaches of security safeguards that pose a real risk of significant harm;
- notify affected individuals and relevant third parties of any breaches with a real risk of significant harm; and
- keep records of all breaches, regardless of whether a breach presents a real risk of significant harm.

Real risk of significant harm

Real risk of significant harm must be determined through an assessment of the sensitivity of the personal information involved, as well as the probability the personal information could be misused.

Significant harm includes:

- bodily harm;
- humiliation, damage to reputation or relationships;
- loss of employment, business or professional opportunities;
- financial loss, identity theft, negative effects on the credit record; or
- damage to or loss of property.

What your breach report to the OPC should contain

A report of a breach of security safeguards to the OPC must be in writing and must include:

- a description of the circumstances of the breach and, if known, the cause;
- when the breach occurred;
- as much as possible, a description of the personal information that is the subject of the breach;
- the number or approximate number of individuals affected by the breach;
- what steps the organization has taken to reduce the risk of harm to affected individuals.
- what steps the organization has taken or will take to notify affected individuals; and
- name and coordinates of a contact person.

What your notification to affected individuals needs to contain

- much of the same information a breach report to the OPC must contain; and
- the steps affected individuals can take to reduce the risk of harm, for example, changing their passwords or monitoring accounts.

What you need to include in your own breach records

The OPC can request to have access to or a copy of an organization's breach records. These records must contain sufficient detail to allow the OPC to determine whether an organization has properly assessed the risk of harm and has met its obligations for reporting and notification of a particular breach.

Records do not need to include personal information unless that information is needed to explain the nature and sensitivity of the breach, or the probability of the personal information being misused.

You are required by the Breach of Security Safeguard Regulations to keep all breach records for two years. You may have other legal requirements to keep them longer.

Related link

- What you need to know about mandatory reporting of breaches of security safeguards

Complaints to the Privacy Commissioner of Canada

An individual may file a complaint under PIPEDA if they feel an organization has violated the law.

The Privacy Commissioner can also initiate a complaint if the Commissioner is satisfied that there are reasonable grounds to investigate a matter.

Complaint process

The Commissioner seeks to take a cooperative and conciliatory approach to investigations whenever possible. The OPC encourages parties to resolve complaints amongst themselves, and may use alternate dispute resolution methods such as mediation and conciliation to settle matters at any stage of the investigation process.

The OPC will review complaints and approach them in one of three ways:

- by attempting to resolve them on an informal basis (known as early resolution);
- by declining to investigate; or
- by deciding to investigate.

Key steps for each of these processes are listed below and are also explained in the PIPEDA complaints and enforcement chart on our website.

Note that it is an offence under PIPEDA to:

- destroy personal information that an individual has requested;
- retaliate against an employee who has complained to the OPC; or
- obstruct an investigation or audit by the Commissioner or his or her delegate.

Early resolution

Complaints that may be resolved informally are handled via an early resolution process. These complaints include matters where:

- it seems possible to easily address the allegations on an informal basis; or
- the parties are willing to resolve the matter informally.

Using this process, the OPC helps to identify a solution that satisfies all parties without a formal investigation. No reports of findings are issued in matters that are resolved informally.

Decline to investigate

The OPC may decline to accept a complaint for investigation if it believes that:

- the complainant should first exhaust other available grievance or review procedures;
- the complaint could be better dealt with through a different procedure provided for under federal or

provincial law (for example, a rental dispute may be better addressed through a landlord-tenant tribunal); or
- the complaint was not filed within a reasonable time period.

When the OPC declines a complaint, it informs all parties of its decision and provides reasons. A complainant may ask that the decision be reconsidered.

If the OPC is satisfied that the complainant has established compelling reasons to investigate, the matter will be referred for investigation.

Investigations

The following process outlines the steps the OPC generally takes when investigating privacy complaints against organizations.

1. When the OPC accepts a complaint for investigation, it assigns an investigator to the file.

2. Once an investigation begins, the OPC provides written notice to the organization explaining the substance of the complaint.

3. The investigator contacts the organization's designated representative to:
   - explain how the investigation will proceed;
   - identify any records that must be reviewed and any staff members who may be interviewed; and
   - indicate whether on-site visits will be needed.

4. The investigator obtains information directly from individuals familiar with the matter under investigation.
   - The investigator may ask the organization to provide information or documents that are relevant to the investigation.
   - If conducting a site visit, the investigator may examine or obtain copies of or extracts of documents, including those stored electronically, that are found in the premises.

5. Prior to finalizing the investigation, the results may be disclosed to the parties involved. This may be done to obtain additional representations, if the parties see fit to provide them, or to give the respondent the opportunity to resolve the matter before the complaint is finalized.

Note: The OPC has the power to summon witnesses, administer oaths and compel people and organizations to produce evidence, as well as conduct site visits.

6. Based on the results of the investigation, the Commissioner or his or her delegate will issue a report to the parties. The report includes:
   - the results of the investigation;
   - any settlement reached by the parties;
   - any recommendations, such as suggested changes in information management practices;
   - the steps the organization has taken or will take to address these recommendations; and
   - notice of recourse to the Federal Court.

7. The Commissioner or his or her delegate can request that an organization provide, 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.

8. The Commissioner may enter into a compliance agreement with an organization if it is believed, on reasonable grounds, that an organization has committed, is about to commit or is likely to commit a contravention of PIPEDA or if it has failed to follow a recommendation related to the 10 fair information principles. Under a compliance agreement, an organization agrees to take certain actions to bring itself into compliance. This would preclude the Privacy Commissioner from commencing or continuing a court application under PIPEDA in respect of any matter covered by the agreement. However, if an organization fails to live up to its commitments, the OPC could, after notifying the organization, either apply to the court for an order requiring the organization to comply with the terms of the agreement, or commence or reinstate court proceedings under PIPEDA as appropriate.

Findings and dispositions

A complaint is normally disposed of in one of several ways.

1. No jurisdiction

Based on the information gathered, the OPC determines PIPEDA does not apply to the organization or activity that was the subject of the complaint. The OPC does not issue a report.

2. Declined to investigate

The OPC may decline to accept a complaint for investigation if it believes that:

- the complainant should first exhaust other available grievance or review procedures;
- the complaint could be better dealt with through a different procedure provided for under federal or provincial law; or
- the complaint was not filed within a reasonable time period.

3. Discontinued

The investigation is discontinued before the allegations are fully investigated. An investigation may be discontinued at the OPC's discretion if:

- there is insufficient evidence to pursue the investigation;
- the complaint is trivial, frivolous or vexatious or is made in bad faith;
- the organization has provided a fair and reasonable response to the complaint;
- the matter is already the object of an ongoing investigation;
- the matter has already been the subject of a report by the commissioner; or
- the complaint was already declined.

4. Withdrawn

The complainant withdraws the complaint voluntarily or cannot be reached. The OPC does not issue a report.

5. Early resolved and settled

Complaints that may be resolved informally are handled via an early resolution process. These complaints include matters where:

- it seems possible to easily address the allegations on an informal basis; or
- the parties are willing to resolve the matter informally.

Using this process, the OPC helps to identify a solution that satisfies all parties without a formal investigation. No reports of findings are issued in matters that are resolved informally.

6. Not well founded

The OPC has determined that the organization did not contravene PIPEDA.

7. Well founded and conditionally resolved

The OPC has determined that an organization contravened PIPEDA. The organization commits to implementing the recommendations made by the OPC and demonstrating their implementation within a specified timeframe.

8. Well founded and resolved

The OPC has determined that an organization contravened a provision of PIPEDA. The organization demonstrates it has taken satisfactory corrective action to remedy the situation, either proactively or in response to recommendations made by the OPC, by the time the finding was issued.

9. Well founded and not resolved

The OPC has determined that an organization contravened a provision of PIPEDA but was unable to resolve outstanding issues.

Compliance agreements

Another possible outcome following a complaint is that the Privacy Commissioner or his or her delegate may enter into a compliance agreement with an organization aimed at ensuring it complies with PIPEDA.

In a compliance agreement, an organization agrees to take certain actions to comply with PIPEDA.

If an organization fails to live up to its commitments in the agreement, the OPC can either apply to the Court for an order requiring the organization to comply with the terms of the agreement, apply for a hearing or reinstitute proceedings, as appropriate.

Audits

PIPEDA gives the OPC the authority to audit an organization's privacy practices when the OPC 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?

Information that can give rise to audit can come from a variety of sources, including:

- a group or series of complaints about a particular organization's practices;
- information obtained during an investigation;
- information provided by an individual under the whistleblower provision; or
- an issue receiving public attention.

Applying for a hearing to the Federal Court

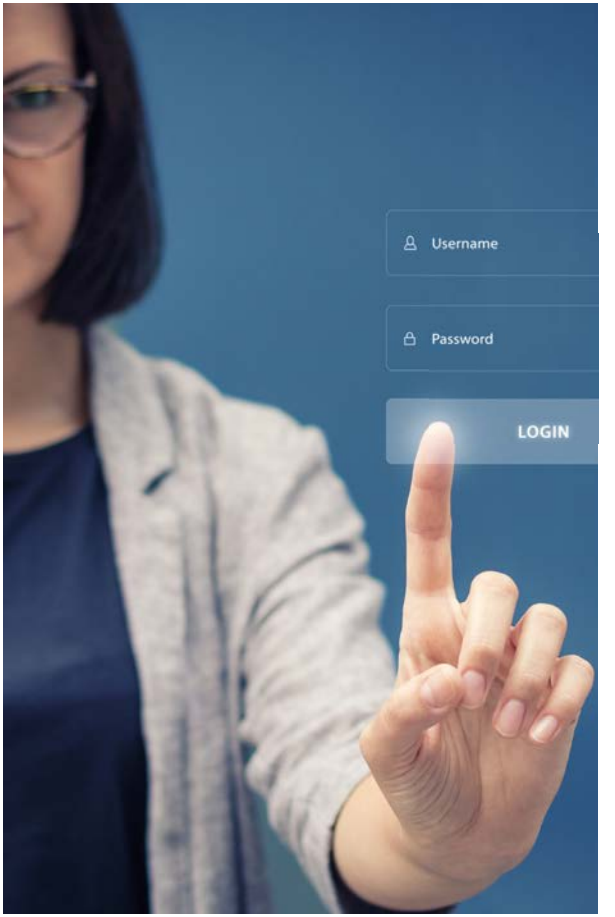
A complainant may apply to the Federal Court for a hearing in certain cases, even if he or she has been notified that an investigation has been discontinued.

The OPC may also apply for a hearing on its own behalf or for a complainant in certain cases.

Any application for a hearing must be made within a year of the OPC's report of findings being released or the OPC's notification that a complaint has been discontinued, though the court may allow a longer period.

Applications to the Court can only be made regarding the matter that the individual complained about or a matter referred to in the OPC's report, and must refer to one of the specific provisions identified in section 14 of the Act.

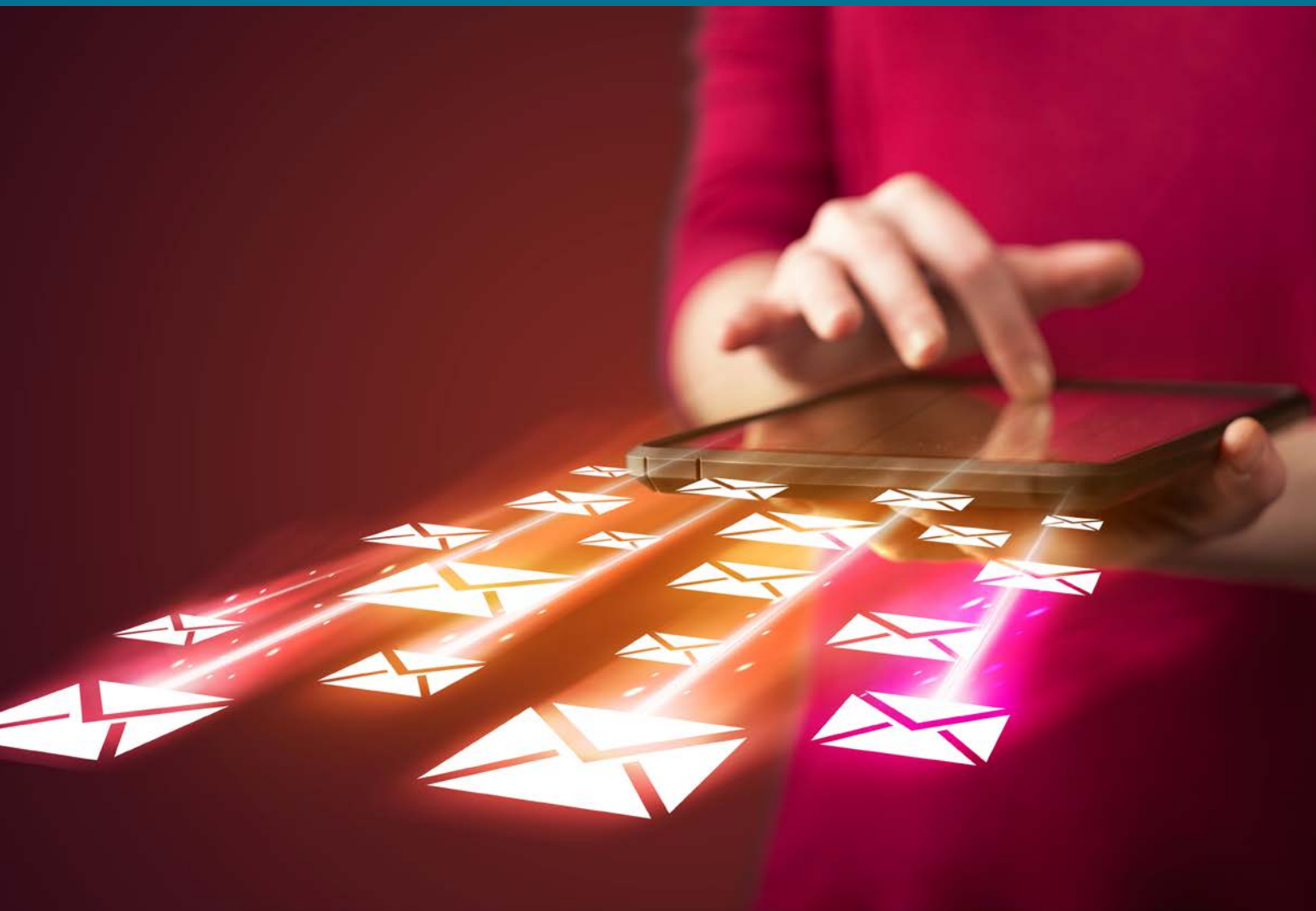
The Federal Court may order an organization to correct practices that do not comply with the Act. It may also order an organization to publish a notice indicating any action taken or proposed to correct these practices. The Court can also award damages to a complainant, including damages for humiliation.



Related link

- How to apply for a Federal Court hearing under PIPEDA

Canada's anti-spam legislation and PIPEDA



Canada's anti-spam legislation **(CASL)** protects consumers and businesses from the misuse of digital technology, including spam and other electronic threats. It also aims to help businesses stay competitive in a global, digital marketplace.

CASL reinforces best practices in email marketing and seeks to combat spam and related issues, such as identity theft, phishing and the spread of malicious software, such as viruses, worms and trojans (malware).

When CASL came into force in 2014, it amended PIPEDA to include new restrictions on electronic address harvesting and collecting personal information using spyware.

The OPC shares the responsibility for enforcing CASL with two other agencies – the Canadian Radio-television and Telecommunications Commission and the Competition Bureau.

The restrictions related to address harvesting are relevant to organizations of all shapes and sizes in all sectors.

An organization has a responsibility to ensure all individuals receiving its electronic messages have provided appropriate consent for the collection and use of their address for marketing and other purposes.

To ensure your organization complies with CASL and to find out how to protect it from cyber threats, visit fightspam.gc.ca or consult our website at priv.gc.ca (search "spam").

Advisory services for businesses

Part of the OPC's role is to help organizations understand their privacy obligations and comply with the law. Our business advisory services can advise you on the privacy impacts of new programs or initiatives.

We can also review how you currently manage privacy to identify good practices as well as potential risks, and give you practical and actionable guidance to help ensure your practices comply with PIPEDA.

The OPC's advisory services for businesses are voluntary and free of charge. All businesses in Canada subject to PIPEDA can request advice. Advisory services are provided based on resource capacity and availability. We prioritize projects with higher privacy risks or broader impacts on Canadians.

For more information, contact:
Office of the Privacy Commissioner of Canada
30 Victoria Street, 8th floor
Gatineau, QC K1A 1H3
Telephone: (819) 994-5444
Toll-free: 1-800-282-1376
TTY: (819) 994-6591
For more information visit: priv.gc.ca/business
Follow us on Twitter: @privacyprivee