PIPEDA legislation and related regulations

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

For more information about the application of PIPEDA, please read our PIPEDA in brief page.

Schedule 1 of PIPEDA contains 10 fair information principles. These principles are referred to throughout the Act.

Administration

Privacy Commissioner of Canada — The Office oversees compliance with PIPEDA. Canadians may complain to the Commissioner about any matter specified in section 11 of PIPEDA. The Commissioner may also personally initiate a complaint.

Innovation, Science and Economic Development Canada (ISED) - The Minister of ISED is responsible for PIPEDA. The minister recommends to the Governor in Council the adoption of Orders in Council under the Act and tables Government bills in Parliament to amend the Act.

Related acts and legislation

Several provincial laws have been deemed substantially similar to the PIPEDA. Under paragraph 26(2)(b), the Governor in Council can exempt an organization or class of organizations, an activity or a class of activities from PIPEDA if the collection, use or disclosure of personal information occurs within a province that has legislation that has been deemed substantially similar to the PIPEDA. This means that wherever the substantially similar provincial law applies, that law applies **instead** of PIPEDA.

- Provincial laws that may apply instead of PIPEDA
- Canada's anti-spam legislation
- The *Digital Privacy Act* and PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA)

PIPEDA fair information principles

Revised: May 2019

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.

PIPEDA Fair Information Principle 1 – Accountability

Reviewed: August 2020

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).

PIPEDA Fair Information Principle 2 – Identifying Purposes

Reviewed: August 2020

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

PIPEDA Fair Information Principle 3 – Consent

Reviewed: August 2020

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.

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 level of protection 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.

PIPEDA Fair Information Principle 4 – Limiting Collection

Reviewed: August 2020

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.

PIPEDA Fair Information Principle 5 – Limiting Use, Disclosure, and Retention

Reviewed: August 2020

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.

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.

PIPEDA Fair Information Principle 6 – Accuracy

Reviewed: August 2020

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.

PIPEDA Fair Information Principle 7 – Safeguards

Reviewed: August 2020
Revised: August 13, 2021

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 generally be considered sensitive, along with information such as ethnic and racial origins, political opinions, genetic and biometric data, an individual's sex life or sexual orientation, and religious/philosophical beliefs;
  - 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.

PIPEDA Fair Information Principle 8 – Openness

Reviewed: August 2020

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.

PIPEDA Fair Information Principle 9 – Individual Access

Reviewed: August 2020

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 understand-able. 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.

PIPEDA Fair Information Principle 10 – Challenging Compliance

Reviewed: August 2020

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.

PIPEDA legislation and related regulations

An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.

Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada enacts as follows:

- The complete version of the Personal Information Protection and Electronic Documents Act (PIPEDA) last amended on June 23, 2015.
- The complete version of PIPEDA that received Royal Assent on April 13, 2000.