

PIPEDA-Personal Information Protection and Electronic Documents Act



Business/Organizations

It is your

Business to Know



Business WHAT IS PIPEDA

& Organizations

PIPEDA is federal government legislation that protects your privacy.

P = Personal

I = Information

P = Protection and

E = Electronic

D = Documents

A = Act

PIPEDA sets rules about personal information that you provide to businesses, and how they handle that information.

This information kit will help businesses and organizations understand their responsibilities under PIPEDA.

B

PERSONAL INFORMATION

WHAT IS "PERSONAL INFORMATION" ?

"Personal information" is a lot of things. These things tell other people about you.

Here are some things that are personal information:

- your name and address
- your email address
- the colour of your skin
- your religion
- whether you are married, single, divorced, or separated
- your sexual preference
- your age, height, weight, blood type
- your medical history, including your disability
- your education
- your income (money), and what things you spend it on
- your banking information, such as your bank account number or your PIN number
- your credit card numbers
- your Social Insurance Number (SIN)

This information identifies who you are.

You must be careful about sharing it! Other people can use this information to hurt you or steal from you. They can even use it to pretend to be you!

Some personal information needs to be shared for business purposes, and also for your employers. PIPEDA tries to balance your right to information privacy and organizations' need to collect information for business reasons.

B

PIPEDA RULES FOR BUSINESS

WHAT BUSINESSES MUST FOLLOW PIPEDA'S RULES?

Most private businesses or organizations involved in "commercial activity" must follow PIPEDA's rules.

Many organizations feel confused. They ask questions like these:

- Do registered charities have to follow PIPEDA?
- If the members of an organization pay a fee, is that a "commercial activity"?
- Our organization has a list of the names of people who gave money to us. If we trade our list to another organization for their list, is that a "commercial activity"?

First, let's explain the meaning of "commercial activity". It means selling, buying, renting, and trading.

Most charity organizations are not involved in commercial activities.

- If your organization charges membership fees, that is not a commercial activity.
- If your organization prints brochures or newsletters, or if it has a website, those are not commercial activities.
- Your organization's advocacy work, your services to your community, your attendance at meetings ... those are not commercial activities.

What about fundraising?

Fundraising is not a commercial activity. If people give money to your organization, and if you make a list of their names and addresses, that is not a commercial activity. But if you trade that list of names and addresses to another organization, that is a commercial activity.

If your organization wants to trade your donor list or your member list to another organization, you must have permission from the people whose names are on the list.

Maybe your list has many, many names. Can you ask every person for permission to trade their name? That's a lot of work! There is an easier way to do it. Your membership paper or your donation paper should have a paragraph explaining that sometimes your organization trades names with other organizations. If the person does not want their name traded, they can make a check-mark in a little box on the paper. Then, if the person puts a check-mark in the box, your organization must take their name out of your list before you trade it.

B

TEN PRINCIPLES

TEN PRINCIPLES

How should businesses and organizations handle personal information? The Office of the Privacy Commissioner of Canada suggests that you follow ten principles. "Principles" are good ideas that help you to do the right thing.

Here are the ten principles suggested by the Privacy Commissioner:

1. Responsibility
2. Purpose
3. Permission
4. Limits on collection
5. Limits on using, sharing, and keeping information.
6. Accuracy
7. Protection
8. Awareness
9. Individual access
10. Complaints procedure

B

PRINCIPLE #1 RESPONSIBILITY

Your business or organization should pick a worker who will be responsible for handling personal information. This person needs training:

to understand the rules,
to make sure the organization follows the rules,
to answer questions about privacy,
to watch carefully if any personal information is traded to other businesses and organizations.

Your organization needs to have rules to protect personal information. These rules, which are called “policies and procedures”, should explain several things including the following:

why you collect personal information,
how you protect the information,
how you make sure the information is correct,
how you respond to complaints and requests,
how you will train your staff about privacy policies.

B

PRINCIPLE #2 PURPOSE

Why are you collecting personal information? How will you use it?

Before you collect the information, you must tell people why and how. You have to answer any questions they might ask.

There are many good reasons for collecting personal information. Here are some examples:

you want to open a new bank account
your business wants to provide benefits to your workers, such as health-care insurance
you want to mail your newsletter to people
you want to reserve a room at a hotel, and the hotel asks for your personal information as a “guarantee” that you will pay for the room.

B

PRINCIPLE #3 PERMISSION

Before you collect the personal information, you must tell people why you are collecting it, and how you plan to use it.

The person giving the information must understand clearly. Your organization has to communicate so the person can understand. If the person wants to communicate by talking, writing, or using Sign language, your organization has to be ready to do it.

Always tell the truth about why you need their personal information.

When the person agrees to give his/her personal information to your organization, you need to make an official proof of the agreement. For example, ask the person to sign a paper that says, "I permit your organization to collect my personal information for this purpose."

You can get permission in a personal meeting, by phone/TTY, by mail, by email, or through the Internet.

B

PRINCIPLE #4: LIMITS ON COLLECTION

Before you start collecting personal information, you must decide exactly which information you need for your purposes.

Don't gather a lot of information that you don't need -- that's wasteful and dangerous. Having lots of personal information is hard for your organization to control and protect.

For example, if you are mailing newsletters, you only need the person's name and address. Don't ask them for information about their age, religion, education, or jobs -- you don't need that information to mail a newsletter.

B

PRINCIPLE #5: LIMITS ON USE

LIMITS ON USING, SHARING, AND KEEPING INFORMATION

Personal information is gathered for a specific purpose. It must be used for that purpose.

When the purpose is completed, you cannot keep the information forever. You must set time limits for keeping it.

For example, your organization might collect names and addresses of its members, so that it can mail its newsletter to them. The membership lasts for one year. After one year, if a person does not want to be a member anymore, you must remove their name and address from your list of members. You cannot use that information anymore.

When the time is up, you must carefully get rid of the information. If the information is on paper, you have to shred the paper. If the information is in an electronic file, you have to delete the file.

B

PRINCIPLE #6: ACCURACY

From time to time, you must check the personal information that your organization or business collected to make sure it is still correct. You also need to make sure you still need the information for the same purpose.

If the information is not needed, you have to get rid of it.

If the information is still needed, you should contact the person and ask if there are any changes, corrections, or updates.

Each time you correct or update personal information, you should write down the date when the correction was made.

B

PRINCIPLE #7: PROTECTION

It is really important to protect personal information from theft, loss, wrong use, or letting it be seen by people who shouldn't see it.

Your business or organization must teach your workers how to protect information.

You should use alarms, filing cabinets that can be locked, passwords, firewalls, or security pass-cards.

B

PRINCIPLE #8: AWARENESS

Tell your customers and workers and volunteers about your rules for handling their personal information. Make sure your rules are clear and easy to understand.

Post them on your website
Print them and post them in your offices
Print them in your newsletters.

Be sure to say who in your organization is responsible for handling privacy.

Be sure to explain how people can ask to see the personal information about themselves that you have in your files.

Be sure to explain how people can complain if they think your organization has personal information that it doesn't really need, or that is wrong (inaccurate).

B

PRINCIPLE #9: INDIVIDUAL ACCESS

Suppose a person asks you if you have any of their personal information.

You must answer truthfully.

You have to explain how your organization uses the information.

You have to say if your organization has shared the information with any other organization or business.

If the person wants to see their information, you must show it to them. You have up to 30 days to show it. Sometimes you can ask for more than 30 days, but it depends on the situation.

If the person looks at the information and tells you it is wrong, you should correct it. If you feel the information is not wrong, and if the person can't prove it is wrong, you should write a note saying that you and the other person don't agree. Then you have to tell the person how to make a complaint to your organization.

B

PRINCIPLE #10: COMPLAINTS PROCEDURE

Your business or organization needs to have a written procedure (rules) for handling complaints. It needs to be simple and clear.

First, write a note explaining the complaint. What is it about? Be sure to write down the date that the complaint was made, too.

Next, send the person a written message saying that you have received their complaint. You can ask them for more details, or ask them to explain the problem more clearly.

Choose a person who is very good at handling complaints. Ask that person to investigate (look into) the complaint.

When the investigation is finished, you must share the results or the report with the person who complained.

If the investigator suggests how to fix the problem, you must share these suggestions with the complaining person. Tell the person if you are going to accept the suggestions. Tell the person when you have finished fixing the problem.

A large, stylized red letter 'B' is positioned on the left side of a light purple horizontal bar that spans across the top of the page. The bar has a rounded right end and a thin black line running through its center.

A FINAL WORD FOR YOU!

Businesses and organizations must know the rules of the PIPEDA. This brochure explains some of the most important points. If you need more detailed information, contact the Canadian Association of the Deaf, or the Office of the Privacy Commissioner of Canada. We're here to help you!

The OPC's Contributions Program is intended to fund independent privacy research and projects. The opinions expressed in this publication are those of the authors and do not necessarily reflect those of the Office of the Privacy Commissioner of Canada.

For more information:

www.priv.gc.ca

www.cad.ca

We thank the Office of the Privacy Commissioner of Canada for funding this initiative.

The Personal Information Protection and Electronic Documents Act

A Guide for Businesses and Organizations

Produced by the
Canadian Association of the Deaf

with support from the
Office of the Privacy Commissioner of Canada



www.cad.ca

Charitable Business No. 10807 5003 RR0001 No. d'entreprise charitable