

What is the Personal Information and Electronic Document Act (PIPEDA) ?

PIPEDA is the Canadian Privacy Legislation which is overseen by the Privacy Commissioner of Canada. This legislation protects personal information with rules for the proper collection, use and disclosure of the personal information in the course of commercial activity.

What is Personal Information?

Personal Information is information about an “identifiable individual.” Examples of personal information:

- Age
- Ethnic Origin
- Opinions
- Loan Records
- Name
- Income
- Disciplinary Actions
- Credit Records
- ID Numbers
- Blood Type
- Employee Files
- Medical Records

Who must comply with PIPEDA?

Effective January 1st, 2004 the Act extends to all organizations who collect, use or disclose personal information in a commercial activity. All businesses, associations, partnerships, persons and trade unions are subject to the terms of the act. Also included is any person or organization who is selling, bartering or leasing of donor, membership or other fundraising lists.

The Act in Brief:

“Organizations covered by the Act must obtain an individual’s consent when they collect, use or disclose the individual’s personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for the purpose for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.”

Your Responsibilities under the Act:

“An organization is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealing with third parties.” The act is divided into 10 principals that businesses must follow. The 10 principals are:

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

These are the two principals that apply to managing your document retention and shredding.
See the next page for a more detailed look at the requirements.

Below is an excerpt from the “Your Privacy Responsibilities, Canada’s Personal Information Protection and Electronic Documents Act” published by the Office of the Privacy Commissioner of Canada.

You can find this guide and the entire act at : http://www.priv.gc.ca/information/guide_e.cfm#012

Principal 5—Limiting use, disclosure and retention

Your Responsibilities:

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

How to fulfil these responsibilities:

- Document any new purpose for the use of personal information
- Institute maximum and minimum retention periods that take into account any legal requirements or restrictions and redress mechanisms.
- Dispose of information that does not have specific purpose or that no longer fulfils its intended purpose.
- Dispose of personal information in a way that prevents improper access. Shredding paper files or deleting electronic records are ideal.
- Establish policies setting out the types of information that need to be updated. An organization can reasonably expect an individual to provide updated information in certain circumstances (e.g. change of address for a magazine subscription.)

Principal 7—Safeguards

Your Responsibilities:

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

How to fulfil these responsibilities:

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

How we can help.

Phoenix provides secure storage of business records and secure shredding programs for both everyday paper shredding and one time service. Please visit our web site at: www.phoenixrecycling.ca or call us at 204-222-5096 to learn more about how we can help you.

Please note that this document is not a legal opinion. This document should not be relied on with out obtaining legal advise.