

What is the Personal Information Protection and Electronic Documents Act?

The Personal Information Protection and Electronic Documents Act (PIPEDA) protects personal information in the hands of private sector organizations and provides guidelines for the collection, use and disclosure of that information in the course of commercial activity. The Act is overseen by the Privacy Commissioner of Canada.

Personal information is defined as “information about an identifiable individual”. For example, name, address, telephone number, gender, ID numbers, income, blood type, credit records, loan records and other information. PIPEDA also covers “sensitive personal information”, such as a person’s health or medical history, racial or ethnic origin, political opinions, religious beliefs, trade union membership and financial information.

Who is affected?

As of January 1, 2004, Canadian organizations engaged in commercial activity are required to comply with the Act’s 10 privacy principles. The Act covers businesses, associations, partnerships and trade unions including organizations engaged in the selling, leasing or bartering of donor, membership or other fundraising lists.

What does PIPEDA have to do with information management?

PIPEDA puts the obligation to safeguard information on the company that collects the information. Organizations that fail to protect the privacy of personal information face significant risks, including legal action industry or regulatory sanctions and, of course, damage to their reputation, brand and business relationships.

More specifically, Schedule 1, Section 5 of PIPEDA outlines 10 Principles. Principles 5 and 7 relate to document retention and destruction:

4.5 Principle 5 – Limiting Use, Disclosure, and Retention – “Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1). Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal

information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.7 Principle 7 – Safeguards – “The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

The methods of protection should include: (a) physical measures, for example, locked filing cabinets and restricted access to offices; (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and (c) technological measures, for example, the use of passwords and encryption.

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).”

What do companies have to do to comply with PIPEDA?

Compliance is addressed throughout the Act. In general, Companies need to have a privacy policy statement, modeled after PIPEDA's ten privacy principles. The policy must address information management practices including collection, use, disclosure, retention, security and destruction.

Ensuring compliance is the responsibility of the Privacy Commissioner of Canada. PIPEDA Part 1, Division 2 addresses the process for filing and investigating non-compliance. Complaints are investigated and, as stated in the section, "the Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation." The Commissioner may also refer issues to the Federal Court for a hearing. Hearings are addressed in Part 1, Division 2, Section 14 to 17. Section 16 addresses remedies:

"16. The Court may, in addition to any other remedies it may give, (a) order an organization to correct its practices in order to comply with sections 5 to 10; (b) order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and (c) award damages to the complainant, including damages for any humiliation that the complainant has suffered."

There is no ceiling on monetary damages that the Court may award. Also, Principle 9 requires organizations to give individuals access to all of their personal information in the organization's control upon request. Organizations must do so within 30 days

How can we help?

Securit provides companies with the security of knowing that their documents are stored safely while still being accessible to those who need them.

Whether disposing of information on a day-to-day basis or at the end of the determined retention period, Securit ensures materials are destroyed completely, on-site, by our Customer Service Representatives. Upon completion, Securit provides a Certificate of Destruction to prove that the documents were destroyed. For peace of mind, For peace of mind, contact Securit today at 1 800 697-4733.

For more information:

Privacy Commissioner of Canada –

<http://www.privcom.gc.ca/>

Industry Canada, Privacy for Business –

<http://privacyforbusiness.ic.gc.ca/epic/internet/>

inpfb-cee.nsf/en/Home

This document does not constitute a legal opinion or legal advice. Do not rely on any of the information in this document without first obtaining legal advice.

© Copyright 2005