

What is the B.C. Personal Information Protection Act?

The Personal Information Protection Act (PIPA) protects personal information in the hands of private sector organizations and provides guidelines for the collection, use and disclosure of that information. The Act is overseen by the B.C. Information and Privacy Commissioner.

Personal information is defined as “information about an identifiable individual”. This includes a person’s name, address, telephone number, gender, ID numbers, income, blood type, credit records, loan records and other information. It also includes 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.

PIPA also covers personal information about organizations’ employees.

Who is affected?

As of January 1, 2004, all organizations (including businesses, associations, partnerships, trade unions and other organizations) which collect, use or disclose any personal information in British Columbia must comply with PIPA.

What does PIPA have to do with information management?

PIPA puts the obligation to safeguard information on the organization that collects the information.

For example, Section 34 of PIPA requires organizations to make reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification and disposal of personal information. Section 35(2) requires organizations to destroy or alter documents containing personal information within specific time-frames. All destruction must be done securely.

Also, Section 23(1) 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.

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.

What do organizations have to do to comply with PIPA?

Organizations need to have a privacy policy statement, modeled after PIPA’s privacy obligations. The policy must address information management practices including collection, use, disclosure, retention, security and destruction.

How can we help?

Securit provides organizations with the security of knowing that their documents are stored safely while still being quickly 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, onsite, by our Customer Service Representatives. Upon completion, Securit provides a Certificate of Destruction to prove that the documents were destroyed. For peace of mind, contact Securit today at 1 800 697-4733.

For more information:

Information and Privacy Commissioner of B.C. – <http://www.oipcbc.ca/>

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

