OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
for
British Columbia

Personal Information Protection Act —
A Summary for Organizations

Please note that, while this summary sets out some of the basic elements of BC's Personal Information Protection Act*, it is for general information only, it is not intended as legal or other advice, and it does not bind or fetter the Office of the Information and Privacy Commissioner for British Columbia (OIPC) in interpreting or applying PIPA. PIPA prevails in all cases and should be referred to. This document was prepared in co-operation with, and with the generous support of, the Office of the Information and Privacy Commissioner for Alberta and the Alberta government, but its contents are the sole responsibility of the OIPC. Further information, useful tools and links to other resources can be found at the OIPC's website, www.oipc.bc.ca. Date of this version: December 30, 2003.*

British Columbia's *Personal Information Protection Act (*"PIPA") describes how your organization must handle its customers' and employees' "personal information". PIPA defines "personal information" as "information about an identifiable individual". PIPA comes into effect on January 1, 2004. This document summarizes some of PIPA's key features.

PIPA applies to all provincially-regulated private sector "organizations". It covers all businesses (such as corporations, partnerships, sole proprietorships and individuals acting as agents or contractors).

PIPA also applies to non-profit organizations, including trade unions, charities, foundations, trusts, clubs, churches and amateur sports organizations.

PIPA does not apply to any "public body" covered by British Columbia's *Freedom of Information and Protection of Privacy Act* or to personal information to which that Act applies.

PIPA does not apply to collection, use or disclose of personal information for domestic, artistic, literary or journalistic purposes. PIPA therefore can apply to all of your organization's activities or only to some (example: a newspaper's use of personal information for a story is not covered, but its use of customer information for subscription purposes is covered).

Your organization's PIPA responsibilities

Your organization is responsible for all personal information under your control. This means you are responsible even for personal information your contractors are using.

Your organization must choose someone to be responsible for compliance with PIPA. You must release the position name or title, and contact information, of the responsible individual.

PIPA uses the "reasonable person test" for deciding whether an organization has carried out its PIPA responsibilities. The test refers to what a reasonable person would think appropriate in the circumstances.

Getting consent to collection of personal information

Your organization needs consent to collect personal information from an individual or another source, and to use and disclose it. There are exceptions to the need to get consent.

PIPA considers consent to be given when an individual, knowing of the purpose of collection of his or her information, gives the information to you.

You should decide, however, whether getting express, written consent is desirable. When deciding on the type of consent, consider what is reasonable for the individual, the circumstances of collection, your proposed uses or disclosures of the information, the sensitivity of the information, and whether you may need to prove that the individual consented.

An individual can change or withdraw consent in some situations, but not if doing so would interfere with a legal obligation.

In some cases, PIPA allows collection without consent, including where you are collecting "employee personal information" that is reasonably needed for starting, managing or ending an employment relationship with the individual; in an emergency; and for an "investigation" or "proceeding", but only if consent would compromise the availability or accuracy of the information collected for the investigation or proceeding.

PIPA regards personal information collected before January 1, 2004 to have been collected with consent, but only for the original purpose for which it was collected.

Rules for collecting personal information

Collect personal information only for reasonable purposes and only collect the amount and type of information reasonably needed to carry out the purposes for collecting it. You usually need to give notice about why you are collecting personal information before, or at the time, you collect the information. Collect directly from the individual unless he or she agrees to someone else giving the information to you.

Rules for using and disclosing personal information

Use and disclose information only for reasonable purposes. As well, only use or disclose the amount and type of information needed to carry out those purposes. PIPA permits using and disclosing without consent for limited and specific circumstances

Employee personal information

PIPA has special rules for "employee personal information" and considers employees to include volunteers. You may collect, use and disclose employee personal information without consent if it is reasonable for starting, managing or ending an employment relationship with the individual involved. You usually need to first give notice to the employee or prospective employee that you are doing so.

Buying or selling a business

When buying or selling a business, you may collect, use and disclose information without consent when those involved agree to do so only for the transaction and when they need the information to decide whether to buy or sell.

Once you complete the transaction, the organization receiving the personal information may continue to use and disclose it, but the information can only be used and disclosed for the purpose for which it was originally collected. Further, the information must relate solely to the carrying on of the business.

If the transaction does not proceed, the organization that received the personal information must destroy or return it.

Requests to obtain your own personal information

Individuals have a right to be given access to their own personal information, to know how their information is or has been used, and to know to whom and in what situations you have disclosed the information. Organizations may charge a minimal fee for access, but cannot charge a fee to their employees for giving access to employee personal information.

In some cases, PIPA authorizes another person to act on behalf of the individual, for example, a parent on behalf of a young child.

Your organization has a duty to help individuals with their requests and to respond within 30 working days. You can extend the response time in certain cases.

In some circumstances, you can or must refuse access to someone's personal information, including where disclosure would harm someone else; would harm an investigation or legal proceeding; when access would disclose someone else's personal information; would disclose confidential business information; or is protected by solicitor-client privilege.

If an individual is not satisfied with what you disclose, he or she may ask the OIPC to investigate.

Correcting personal information

Individuals have a right to ask your organization to correct their personal information if your records contain errors or omissions.

You must correct any error or omission and, if reasonable, inform other organizations to which you have disclosed the incorrect information. You are not required to correct opinions.

If you decide there is no error or omission, you must annotate the record with the requested correction that you did not make.

If an individual is not satisfied with your decision, she or he can ask the OIPC to review the matter.

Accuracy, protection and retention of personal information

If you are likely to use personal information to make a decision affecting the individual, take reasonable steps to ensure the information is accurate and complete.

Use reasonable safeguards to protect personal information from theft, modification, unauthorized access, collection, use, disclosure and destruction. Safeguards should be appropriate to the sensitivity of the information.

Only keep information for as long as reasonable to carry out business or legal purposes. Use care in disposing of, or destroying, information.

Oversight

Individuals may complain to the OIPC if they consider their personal information has not been collected, used or disclosed as required by PIPA, that their personal information is not accurate or complete, or that their request for access or correction has not been handled properly.

The OIPC can investigate complaints it receives. It can also initiate its own investigation where reasonable grounds exist to believe an organization is not complying with PIPA. The OIPC will generally require a would-be complainant to first try to work out a solution directly with the organization involved, without OIPC involvement. The OIPC will try to mediate a settlement of any complaint that it does accept. It may hold a formal inquiry into a complaint that has not settled. The OIPC can compel testimony, order production of evidence and enter premises to investigate a matter.

The OIPC can issue binding orders and can publish its orders. Organizations have 30 working days to comply with an order unless they ask the BC Supreme Court to overturn the order before the 30-day period expires.

PIPA creates various offences, including using deception or coercion to collect personal information contrary to PIPA; disposing of personal information with an intent to evade a request for access to that personal information; obstructing the OIPC; and failure to comply with an OIPC order. There are fines of up to $10,000 for individuals and up to $100,000 for organizations. Individuals may sue you for damages they actually suffer due to your failure to comply with PIPA.