

3200 Vancouver Centre,

650 West Georgia Street

Vancouver, B.C. Canada

V6B 4P7

www.hgelaw.com



Law Bulletin

January 2004

*Prepared by Barbara Norell.
Harper Grey Easton*

Harper Grey Easton

BC's Litigation Law Firm



Private sector organizations must be aware of this important new legislation and steps they should take to comply with it.

*Personal Information Protection Act
Prepared by Barbara Norell, Harper Grey Easton*

On January 1, 2004, B.C.'s new privacy legislation, the Personal Information Protection Act (PIPA) became law. PIPA has the potential to dramatically change the manner in which organizations conduct business in B.C. It may affect an organization's relationships with its customers, clients, employees, contractors and other businesses. Private sector organizations must be aware of this important new legislation and steps they should take to comply with it.

The following briefly outlines the requirements of PIPA for organizations generally. PIPA applies to the wide spectrum of the private sector, from construction companies to accountants, and from restaurants to insurers. Out of necessity, it contains general principles. How those general principles apply will depend on many factors such as: the nature of the relationship between an organization and the individuals from whom it is collecting information; the type of personal information collected and whether there are already in place sectoral privacy codes or guidelines or legislation that regulates that organization.

Scope
PIPA applies to every "organization" in B.C. which subject to some exceptions, includes a "person, an unincorporated association, a trade union, a trust, or a not for profit organization." It does not apply to the collection, use or disclosure of personal information by an individual solely for his or her personal or domestic purposes.

Two important exceptions concern the applicability of other legislation. First, PIPA does not apply to

personal information or "public bodies" that are subject to B.C.'s public sector privacy legislation, the Freedom of Information and Protection of Privacy Act. PIPA applies to the private sector.

The second important exception is that PIPA does not apply to the collection, use or disclosure of personal information if the federal private sector privacy act, PIPEDA, applies. As of January 1, 2004, PIPEDA applies to organizations within provincial jurisdiction that collect, use, or disclose information across provincial boundaries in the course of commercial activity. As of that date it also applies to organizations within provincial jurisdiction that collect, use, or disclose information within provincial boundaries in the course of commercial activity unless the province has enacted what the Governor in Council determines is "substantially similar" privacy legislation.

PIPA is B.C.'s response to the "substantially similar" privacy legislation requirement. There is a debate as to whether the legislation will be considered to be substantially similar. The former federal privacy Commissioner has stated that in his view there are deficiencies so that it does not meet this requirement. Industry Canada is responsible for making recommendations to the Governor in Council as to whether or not to approve the legislation as substantially similar and has not yet commented.

Although PIPA and PIPEDA are quite different in structure, on the whole they both embody the same privacy principles. These principles are the nuts and bolts of what organizations need to know about their privacy obligations. Either through PIPA or PIPEDA, private sector organizations will be required to comply with these principles which are discussed below.



PIPA applies to personal information which is defined as “information about an identifiable individual”

Personal Information

PIPA applies to personal information which is defined as “information about an identifiable individual” (a natural person). This definition is very broad and would include a vast array of information. There are several exceptions. Personal information does not include contact information—essentially business card information—or work product information. Work product information is defined in the act.

Because PIPA states that personal information is about an “identifiable individual” it does not apply to data that has been made anonymous and cannot be linked to an individual.

PIPA does not apply to the collection of personal information that is collected prior to the act coming into force. However it applies to the use and disclosure of this information: the personal information may be used and disclosed to fulfil the purposes for which it was collected.

Purpose of Act and Overriding Principle

PIPA seeks to balance two competing interests: “the right of individuals to protect their personal information and the need of organizations to collect, use, or disclose personal information.”

It adopts an overriding reasonable person test: an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances, and that fulfill the purposes described or are otherwise permitted under the Act.

Identifying Purposes and Consent

PIPA prohibits the collection, use, or disclosure of personal information about an individual except when:

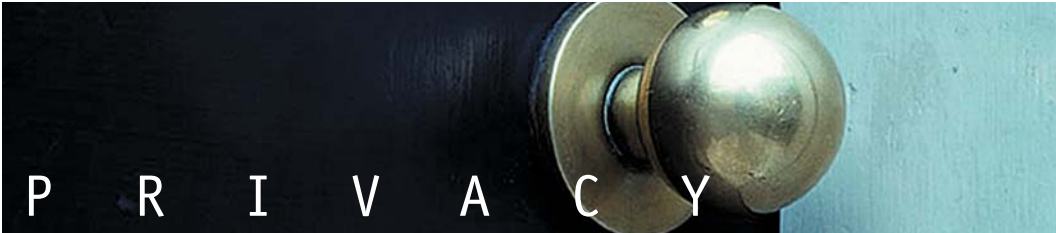
- the individual gives consent; or
- the act deems there to be consent; or
- the act authorizes the collection, use, or disclosure without consent.

Subject to the deemed consent provisions, an organization must disclose to an individual verbally or in writing, the purposes for the collection of the personal information at or before the time of collection. Any consent obtained without disclosing the purpose is not a valid consent. Similarly, any consent obtained through the provision of false information or the use of misleading practices is not a valid consent. A person should be able to reasonably understand how the information will be collected, used, or disclosed.

Consent cannot be coerced. An organization cannot refuse to provide a product or service to an individual because the individual would not provide consent to the collection use or disclosure of personal information if that information is not truly required to provide the product or service.

Consent may be withdrawn subject to certain restrictions and reasonable notice. If an individual withdraws consent the organization must advise him or her of the effect of the withdrawal.

If an organization wants to use information that it has previously collected for a new purpose, it must identify that new purpose and obtain the individual’s consent prior to using the information for the new purpose.



There are several exceptions to the consent principle and organizations will need to look at the particular wording of each.

The act has a section entitled “Implicit consent” which provides that consent will be implied in three sets of conditions. Under the first set of conditions, an individual is deemed to consent to the collection, use or disclosure of personal information for a purpose if the purpose would be considered to be obvious to a reasonable person, and the individual voluntarily provides the information for that purpose. An example would be the provision of credit card information for the purpose of billing.

Under the second set of conditions, an organization may collect, use or disclose personal information for a purpose if: it provides the individual notice that it intends to collect, use or disclose information for that purpose; the individual has a reasonable opportunity to decline; the individual does not decline; and the collection, use or disclosure is reasonable having regard to the sensitivity of the information in the circumstances. An example would be providing notice stating that customer name and address will be used for a certain marketing purpose unless the customer declines.

The third set of conditions concerns collection of information for enrollment of a beneficiary or insured under an insurance, pension or similar plan.

Other than the “Implicit consent” provision, PIPA is silent on the form of consent that is required or that would be appropriate in any given circumstance save for the overriding requirement that an organization must consider what a reasonable person would consider appropriate.

Employee Personal Information

PIPA makes a distinction between personal information and employee personal information,

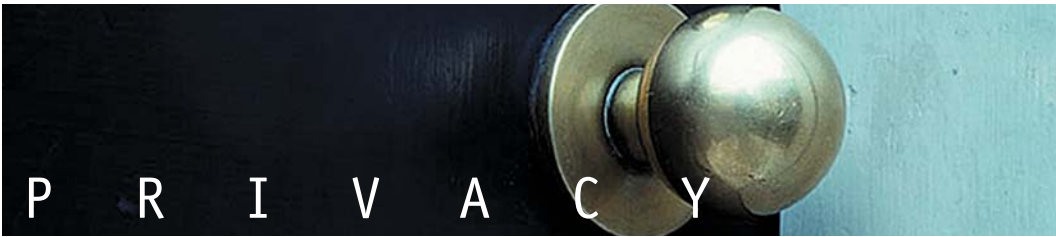
which is defined in the act. Employee personal information is a subset of personal information. There are special provisions addressing the collection, use or disclosure of employee personal information. Under PIPA, an employee includes a volunteer.

An organization may collect, use and disclose employee personal information without the consent of the individual if the collection is reasonable for the purposes of establishing, managing or terminating the employment relationship and prior notification is given to the employee.

Exceptions to Consent Requirement

PIPA provides exceptions where personal information, including employee personal information, may be collected about an individual from a third party, or where the consent of an individual is not required for collection, use or disclosure of the individual’s personal information. There are several exceptions and organizations will need to look at the particular wording of each. Examples of some of the exceptions are when the collection, use or disclosure:

- is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- is reasonable for an investigation or a proceeding (both defined in PIPA), and the consent of the individual would compromise the availability or accuracy of the personal information (for collection) or would compromise the investigation or proceeding (for use or disclosure)
- is of publicly available information from prescribed sources;
- is required or authorized by law;
- is necessary for the collection or payment of a debt;



PIPA provides that an organization must make reasonable efforts to ensure the personal information it collects is accurate and complete.

- is by another organization who is carrying out work on behalf of the organization if certain conditions are met;
- is to comply with a subpoena, warrant or order;
- is to a lawyer representing the organization.

Sale of an Organization or its Assets

PIPA has a section providing for the collection, use or disclosure of employee, customer, director, officer and shareholder personal information in the context of an actual or prospective sale, purchase, lease, merger, amalgamation, or financing of an organization. Collection, use or disclosure without consent of personal information to and from a party or prospective party is permitted when certain conditions have been met.

Access to and Correction of Personal Information

PIPA provides that an organization must make reasonable efforts to ensure the personal information it collects is accurate and complete.

Upon request, an organization must provide an individual with the individual's personal information under its control, information regarding the ways in which the information has and is being used, and to whom it has been disclosed. Organizations will need a system to record when and to whom information was used or disclosed.

Applications for access to personal information must be made in writing. The organization must respond within 30 days except in limited circumstances when the time period may be extended. If access is denied to all or part of the personal information, the reasons must be stated again except in limited circumstances.

Organizations may charge a minimal fee for access to or copying of personal information that is not employee information so long as the individual is advised of this before providing the information.

There are exceptions to an individual's access rights. Organizations will need to look at the particular wording of each exception. Organizations may refuse to disclose personal information in certain situations, including the following:

- it is protected by solicitor-client privilege;
- the disclosure would reveal confidential commercial information;
- it was collected under the "investigation or proceedings" exception

Organizations are prohibited from disclosing personal information if:

- the disclosure would reveal personal information about another individual;
- the disclosure would reveal the identity of an individual who has provided personal information about another, and the individual does not consent to disclosure of his/her identity.

The above exceptions do not apply if the information can be severed from the information.

Individuals may request that errors or omissions in their personal information be corrected. If the correction is not made, a note of the request must be made. If a correction is made, the corrected personal information must be sent to each organization to which the personal information was disclosed in the prior year.

Care of Personal Information

PIPA provides that an organization is responsible for information under its control, including personal



PIPA provides that an organization is responsible for information under its control, including personal information that is not in its custody.

information that is not in its custody. The information must be protected by “reasonable security arrangements to prevent access, collection, use, disclosure, copying, modification or disposal or similar risks.”

Although not specifically addressed in PIPA, contractual terms with third parties may be required to meet reasonable security arrangements for information that is in an organization’s control but not custody.

Sensitivity of the information will be a factor in considering what is reasonable in any given circumstances. If records are stored on paper, locked storage cabinets may be required. If information is stored electronically, other measures such as passwords or encryption may be required. Threats to personal information may come from within and outside an organization. Further, threats are not necessarily intentional; for example, the accidental corruption of electronic records.

Organizations must consider security of personal information when disclosing the information. This is important with the use of electronic and fax transmissions

Care must be used in the destruction of records. If the information is sensitive, shredding may be necessary before disposal or recycling. If electronic records are used, organizations must ensure that deleted records cannot be reconstructed.

Organizations should have a retention policy with minimum and maximum periods. PIPA requires that information be retained only for as long as it is required for the purposes collected, and it is no longer necessary for legal or business purposes.

There is a minimum retention period of one year after personal information has been used. Organizations will want to consider statutory limitation periods in setting their retention policy.

Accountability and Openness

PIPA provides that an organization must designate an individual(s) who is responsible for the organization’s compliance with the act. In a large organization this may be a privacy officer, but in smaller organizations, logical persons might be the owner or the office manager. This individual and the individual’s contact information must be identified upon request by the public.

An organization must develop and follow policies and practices necessary to fulfil its obligations under the act. This includes establishing a complaint procedure and making information available upon request concerning this and its privacy policies and practices. In many situations, a written privacy policy or brochure will be appropriate.

Challenging compliance, complaints to the Commissioner and remedies

If an individual feels that an organization has not complied with PIPA, he or she must be able to address that challenge to the organization’s privacy officer. Organizations are required to put in place a complaints procedure. The organization must take appropriate measures to address the complaint.

The provincial privacy commissioner is given powers to receive complaints and conduct investigations, audits, inquiries and reviews of organizations and their privacy practices. The commissioner has order-making powers. There is a right of judicial



*Organizations
are required to
put in place a
complaints
procedure.*

review. There are offence provisions with fines of up to \$100,000.

If the commissioner has made an order against an organization, or an organization has been convicted of an offence under PIPA, an individual affected by the order or conduct of the organization has a cause of action against the organization for damages for “actual harm” that the individual has suffered.

Industry Codes of Conduct and other enactments

Many organizations are already subject to sectoral privacy codes or guidelines, or legislation that although not called privacy legislation, protects privacy interests. Those works should be considered by organizations when addressing their privacy obligations under PIPA.

How we can assist: Further information

If you would like further information or assistance with identifying potential privacy issues for your organization, or have particular questions you would like addressed, please contact Barbara Norell, at 604 895 2832 or bnorell@hgelaw.com