The Personal Information Protection and Electronic Documents Act

© 2003, Bruce D. Margles

Bruce D. Margles is a business lawyer and corporate counsel practicing in Richmond Hill, Ontario. He can be reached at: Tel: 905-709-7417 or by e-mail bmarglesthompsonlaw.ca.

The Personal Information Protection and Electronic Documents Act

The Personal Information Protection and Electronic Documents Act (the “Act”) was enacted in response to advances in information technology and a growing public concern for the protection of the personal, financial and health information. There was also a perceived need for more reliable and standardized treatment of e-commerce and electronic documents. Through the end of this year, the Act’s application in general has been limited to private-sector organizations that are federally regulated within Canada, and those Canadian firms transferring personal information outside of Canada for a fee.

On January 1, 2004, the final phase of the Act will come into full force. This phase will have the most profound effect on how commercial organizations must manage private information that is collected by them.

All companies collect personal information from many sources, including their customers and their employees. In general, the Act stipulates that such companies must obtain an individual’s consent in order to collect, use or disclose the individual’s personal information. An organization that collects personal information must provide these individuals with the right to access any personal information they hold and to be given fair opportunity to challenge such information. Personal information may only be used for the purposes to which it was collected and to which consent was given, and further consent must be obtained from the individual to use his or her personal information for any other purpose.

What is personal information?

Personal information is defined in the Act as any factual or subjective information, recorded or not, about an identifiable individual. It includes personal information in any form, including age, name, any numbers that can be used to identify the individual, income information, ethnic origin, blood type, social status, employee file, credit record, loan record, medical record, consumer dispute, and includes any personal information that is contained in any evaluation, comment, opinion, disciplinary action, dispute or intentions (for example, to acquire goods or services or change jobs). Commercial activity covered by the Act includes any transaction or conduct of a commercial nature, including the selling, bartering or leasing of donor, membership or other fundraising lists. Personal information that is exempted from the Act include the name, title, business address or telephone number of an employee of an organization, and such information
remains unprotected by the Act. Also exempt is the collection, use or disclosure of personal information strictly for personal purposes (such as a personal greeting card list).

**Offences and Penalties**

It is an offense under the Act, with applicable fines of up to $100,000, to:

(i) destroy personal information that an individual has requested;
(ii) retaliate against an employee who has lodged a complaint to the Privacy Commissioner, or to retaliate against an employee who refuses to contravene Sections 5-10 of the Act; or
(iii) obstruct a complaint investigation or an audit by the Privacy Commissioner.

**The Ten Principles of Fair Information Practices**

Private sector organizations must not only abide by the following principles of Fair Information Practices, but they must also ensure that those to whom they transfer personal information abide by these principles.

The ten principles are:

**Accountability**

Every commercial organization must appoint an individual to accept responsibility for compliance with the Act. This individual’s responsibilities include the protection of all personal information collected by the organization or transferred to third parties for processing, and the development and implementation of personal information policies and practices.

**Identifying Purpose**

Commercial organizations must identify the reasons for collecting personal information before or at the time of collection, document why the information is being collected, inform the individual from whom the information is collected why it is needed, and ensure that the purposes are limited to what a reasonable person would expect under the circumstances.

**Obtain Consent**

Individual consent must be obtained before or at the time of collection and whenever a further use for the personal information is identified. Consent may not be made a condition for the supply of a product or service, unless the information is required to provide the product or service. Express consent is usually required, though in the case of non-sensitive data, the reasonable expectations of the data subject may be used in determining whether the consent of the individual may be implied. Employees who collect personal information must be able to answer the individual’s questions about the purposes of the collection.
**Limiting Collection**

Personal information must only be collected to the extent necessary for the purposes identified. Individuals must not be misled or deceived about the reasons for collecting personal information.

**Limiting Use, Disclosure and Retention**

Private sector organizations must put guidelines and procedures into place for retaining personal information. These include instituting maximum and minimum retention periods that take into account legal requirements or restrictions and redress mechanisms, and destroying information that is no longer required in a way that prevents improper access (such as shredding and electronic erasures).

**Maintain Accuracy**

Private sector organizations are responsible for minimizing the possibility of using incorrect personal information through adopting such techniques as checklists that list specific items of personal information required to provide a service; identify the location where all related personal information can be retrieved; record the data when the personal information was obtained or updated; and record the steps taken to verify the accuracy, completeness and timeliness of the information.

**Establish Safeguards**

Personal information must be protected against loss or theft, unauthorized access, disclosure, copying, use or modification through a company security policy that includes, as appropriate, physical and technological protections, as well as organizational controls.

**Openness**

Private sector organizations must make their privacy policies and practices understandable and easily available, including advising the public of the identity of their privacy officer and how to get in touch with that person.

**Access**

In general, individuals must have access to all information held by an organization about them at no or minimal cost within thirty days of receiving a request for access, unless the information comes under one of the Act's statutory exceptions, such as information disclosed to law enforcement, information covered by the attorney-client privilege, cases where disclosure could harm an individual's life or security, and (under certain circumstances) confidential commercial information.
Challenging Compliance

Private sector organizations covered by the Act must develop simple, easily accessible complaint procedures, investigate all complaints received, and take appropriate measures to correct information handling practices and policies in light of complaints.

Although the Act as it applies to private sector organizations comes into effect on January 1, 2004, an organization may retain personal information collected prior to January 1, 2004. However, the organization is prohibited from using such information without obtaining the individual’s consent. Therefore, unless consent is clearly implied or the information is exempted from the Act, no private sector organization may use or disclose this information without the express consent of the individual.


More detailed information on the Act, is available at: www.privcom.gc.ca/information/guide_e.asp.

If you have any questions about the Act, and how it may impact on your business, please contact me, and I would be please to assist you.