GET READY FOR COMPLIANCE WITH PRIVATE SECTOR PRIVACY LEGISLATION

...PIPEDA IS COMING YOUR WAY!

What is PIPEDA?

The Personal Information Protection and Electronic Documents Act (PIPEDA) provides Canadians with a right of privacy with respect to their personal information that is collected, used or disclosed by an organization in the private sector in the course of commercial activity. For the purpose of PIPEDA, personal information is any information about an identifiable individual, other than that an individual’s name, title, business address or telephone number as an employee of an organization. The definition of “organization” is very broad and includes an association, a partnership, a person (which includes a corporation as well as an individual) and a trade union. Commercial activities to which PIPEDA apply may be activities of a one-time or ongoing nature having a commercial character and also include the selling, bartering or leasing of donor, membership or other fundraising lists. To the extent that provincial and municipal government institutions or not-for-profit organizations engage in any activities that have a commercial character, it is possible that they will also be subject to the privacy protection provisions of PIPEDA.

Although PIPEDA has been in force since January 1, 2001, it has not attracted much public attention until recently. This is because its initial application was largely limited to federally-regulated organizations, such as those operating in the telecommunications, broadcasting, banking and inter-provincial transportation sectors. Organizations engaged in commercial activities in these sectors are, for the most part, large and sophisticated entities with sufficient resources to familiarize themselves with PIPEDA and develop timely compliance strategies.1

What is significant about January 1, 2004?

On January 1, 2004, PIPEDA will also apply to every provincially-regulated organization engaged in commercial activity, unless the federal government exempts a province from the application of PIPEDA on the basis that the legislature of a province has enacted legislation that is substantially similar to PIPEDA with respect to the collection, use and disclosure of personal information occurring within that province. To date, only the private sector privacy legislation of Quebec has been found to be substantially similar to PIPEDA. Accordingly, PIPEDA is expected to apply to the intra-provincial commercial activities of organizations in every other Canadian province as of January 1, 2004. Such organizations range from small “mom and pop” operations to very large multi-national companies and all of them will be held to the same standard of compliance.

---

1 PIPEDA has also applied to personal information about employees of federally-regulated entities and to inter-provincial and international trade in personal information since PIPEDA came into force.
How does the Model Code for the Protection of Personal Information fit in?

The privacy-related provisions of PIPEDA are based on the Canadian Standards Association’s Model Code for the Protection of Personal Information (Code). The Code contains the following ten principles (as implicitly modified by PIPEDA):

- **Accountability** - an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization’s compliance with the remaining principles;

- **Identifying purposes** - the purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected;

- **Consent** - the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information;

- **Limiting the collection** - the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means;

- **Limiting Use, Disclosure and Retention** - personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes;

- **Accuracy** - personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used;

- **Safeguards** - personal information shall be protected by security safeguards appropriate to the sensitivity of the information;

- **Openness** - an organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information;

- **Individual Access** - upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate;

- **Challenging compliance** - an individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization’s compliance;
Are there exceptions to the application of PIPEDA?

There are some exemptions to the application of PIPEDA. For example, PIPEDA does not apply to any individual where the personal information collected, used or disclosed by the individual is solely for domestic purposes. It also does not apply to organizations that collect, use or disclose personal information solely for journalistic, artistic or literary purposes, although curiously, no exemption is provided for those who provide personal information to organizations for such purposes.

PIPEDA also recognizes certain exemptions from the requirement for consent to the collection, use and disclosure of personal information in certain circumstances, including law enforcement and emergencies in which people’s lives or safety could be at risk. Other exceptions also exist.

What remedies does an individual have for a breach of PIPEDA or the Code?

An individual may file a written complaint with the Privacy Commissioner of Canada (PCC) against an organization for a contravention of the privacy provisions of PIPEDA or for the organization’s failure to follow a recommendation set out in the Code. The PCC has significant powers that it may employ to investigate and to attempt to resolve the complaint. Normally, the PCC has one year from the date on which a complaint is filed to prepare a report that includes the Commissioner’s findings and recommendations, any settlement reached by the parties, any request for the organization to take a particular action within a specified time or to provide reasons why no such action has been or is proposed to be taken, and the recourse available to the Federal Court of Canada.2

An unresolved dispute may be taken to the Federal Court of Canada (Court) and this must normally be done within 45 days of the date that the PCC sends the report regarding the complaint to the complainant. In addition to the usual remedies available to it, the Court can also order an organization to correct its personal information management practices so as to comply with PIPEDA, order an organization to publish a notice of any action taken or proposed to be taken, and may award damages to the complainant, including damages for any humiliation that the complainant may have suffered.

Are there any penalties for non-compliance with PIPEDA?

Under PIPEDA, the integrity of the PCC’s investigation process and whistleblowers are protected by a scheme that makes it an offence to interfere with an investigation or audit by the PCC or the PCC’s delegate or to dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee or independent contractor who in good faith is a whistleblower with regards to the organization’s lack of compliance with the privacy protection provisions of PIPEDA. Fines of up to $100,000 may be levied against persons committing such offences.

2 As a separate matter, the PCC also has the authority to make public any information relating to the personal information management practices of an organization, and to conduct audits of the personal information management practices of organizations.
How should an organization prepare for PIPEDA?

Organizations that are provincially regulated must be ready to comply with PIPEDA by January 1, 2004. In order for an organization to properly prepare for PIPEDA, the following steps are recommended:

i) Appoint a Chief Privacy Officer (CPO)

The first step is to appoint a Chief Privacy Officer (CPO) to oversee the organization’s compliance. The CPO should ideally be a member of the executive team, so as to ensure that the organization’s compliance with its privacy-related obligations is taken seriously at all levels of the organization.

ii) Assemble a privacy team

The CPO should assemble a privacy team comprised of people from various disciplines required to ensure compliance with PIPEDA. Operational staff, IT staff and personnel with privacy expertise and/or outside consultants will often be part of the team. The team, under the guidance of the CPO, will then design and implement a privacy compliance plan.

iii) Conduct a privacy audit

It is imperative for the organization to conduct a privacy audit at the outset. Questionnaires and business process diagrams are very useful tools for performing such an audit.

What information is collected, and why?

- The first step of the audit is to identify the types and volumes of personal information collected, used or disclosed by the organization and the purposes for which this is done, as well as how and by whom these activities are performed. The organization should consider what consents exist for these activities, remembering that PIPEDA contains no grandfathering provision. In other words, compliance with PIPEDA as of January 1, 2004 is required even with respect to personal information in the possession of the organization on that date that was collected, used or disclosed by the organization prior to that date.

Consent

- Where adequate consent has not been previously obtained for the collection, use and disclosure of personal information from third parties, such consent should be obtained. The consent sought should be what a reasonable person would consider appropriate in the circumstances and limited to the purposes for which the consent is actually required by the organization. Organizations should resist the temptation to over-collect information. A change in the purpose for which personal information is used will require a new consent. Consent should be obtained explicitly whenever possible, especially where the nature of the personal information is sensitive, such as, for example, in the case of financial or personal health information. Opt-out consents should usually be avoided. Organizations may not disclose personal information in their possession to other entities as a matter of business convenience, including affiliates or subsidiaries, without obtaining consent for such disclosure. Organizations should also be aware that they remain responsible for compliance with PIPEDA when they employ third-party organizations to process personal information, and so they should employ appropriate contractual safeguards in these situations.
Protecting personal information - Another aspect of the audit is assessing how personal information is protected within the organization. For example, are physical records containing personal information kept in locked cabinets or offices? Are the IT systems of the organization sufficiently secure to prevent unauthorized access to personal information? What business practices are in place to protect the privacy of personal information? Is personal information kept separate from other types of information? How long is personal information kept by the organization and what disposal means are employed when it is no longer required.

Analyze audit results - The results of the audit should be compared to the requirements of applicable privacy legislation, and privacy impacts and risks should be assessed. The results of the audit will drive the balance of the privacy compliance plan activities, including the remedying of any deficient practices and systems.

iv) Complete the privacy compliance plan

After the audit is completed, the organization should use the results to complete it’s privacy compliance plan.

Draft a privacy code - The organization should draft a privacy code that is made available to the public upon demand. The privacy code should also be posted on the organization’s website. The organization should also draft procedures for implementing its privacy code and handling privacy breaches.

Develop policies and procedures - Processes also have to be in place to enable the organization to respond to public enquiries regarding the organization’s personal information management practices, to requests made by individuals for access to and correction of their personal information (usually within thirty days) and to complaints.

Training - The organization must also ensure that employees are properly trained to carry out the organization’s responsibilities in the area of privacy protection, including compliance with PIPEDA, and with the organization’s privacy code and procedures.

Determine accountability - Finally, the organization must ensure there is an internal accountability mechanism and monitor ongoing compliance as commercial activities evolve. Periodic reviews and audits are useful in maintaining the integrity of the organization’s privacy compliance plan.

What about employer-employee relationships?

Although PIPEDA does not require compliance by employers under provincial jurisdiction with respect to the collection, use or disclosure of personal information of employees, it may be a good idea for any organization embarking on compliance with PIPEDA to treat employee personal information as if PIPEDA applies to it. In addition to possible efficiency gains and building employee trust, adopting such practices may anticipate provincial legislative changes that may confer privacy protection on personal information of employees. If the organization has to construct a privacy compliance infrastructure, it may be desirable only to go through the exercise once.
PIPEDA – Burden or Opportunity?

Although compliance with PIPEDA may seem to be onerous at the theoretical level, in practical terms, compliance will be less difficult for small organizations with simple business processes that make limited use of personal information.

Whatever the size of an organization, compliance can also bring benefits to the organization. First, constructing a privacy compliance plan and conducting a privacy audit may reveal business process inefficiencies and information clutter that when addressed can improve the efficiency and/or profitability of the organization. Second, taking privacy obligations seriously can help an organization build a reputation as a trustworthy supplier, which is an essential element of a customer relationship management strategy.

For further information contact:

Christian S. Tacit
Tel: (613) 231-8333
E-mail: christian.tacit@nelligan.ca