CRAWFORD CHONDON & ANDREE LLP

Management Labour & Employment Lawyers

The Employers' Edge

BULLETIN: JANUARY 2004

Private Sector Privacy Legislation now in force in Ontario

Effective January 1, 2004, every organization which handles personal information in the course of commercial activities will be regulated by the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). Fundamentally, subject to limited exemptions, PIPEDA requires organizations to obtain consent before handling the personal information of individuals. Personal information is very broadly defined in the legislation as any information that identifies an individual, with the exception of information that identifies a person in his or her professional/business capacity; that is, the person's name, position and business contact information. Organizations are required to seek consent before or at the time that the personal information is collected, and must make reasonable efforts to ensure that the individual is advised of the purposes for which the information will be handled. An individual's consent may be either express or implied, however, organizations must obtain express consent when handling "sensitive" personal information such as financial or health information of individuals.

Employee Personal Information

Since January 2001, federally regulated employers have been governed by PIPEDA with respect to how they handle personal information, including personal information of employees. While provincially-regulated organizations are now regulated by PIPEDA when they handle personal information in the course of commercial activities, because PIPEDA is federal legislation and for reasons related to federal/provincial division of powers under the *Constitution Act, 1867*, PIPEDA will not govern provincially regulated employers when they handle employee personal information in the employment context. However, because PIPEDA broadly defines commercial activity as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character", certain activities, such as those related to the sale of a business, could require employers to handle employee information in a manner that is compliant with PIPEDA. Therefore, employers should be mindful that certain uses and disclosures of employee personal information occurring outside the normal administration and functioning of the employment relationship could trigger PIPEDA regualtion.

Further, PIPEDA holds organizations accountable for "information that has been transferred to a third party for processing", and requires organizations to "use contractual or other means to provide a comparable level of protection while the information is being processed by a third party". Accordingly, an employer's disclosure of employee personal information to third parties, such as payroll services, Employee Assistance Plan providers and outplacement firms, will likely be caught by the legislation. Similarly, organizations such as employment agencies and recruiting companies will also be required to ensure that all third parties to which personal information is disclosed are bound by agreements that require them to ensure that they will handle the information in a manner compliant with PIPEDA.

2 County Court Blvd.
Suite 430
Brampton, ON
L6W 3W8
Tel: (905) 874-9343
Fax: (905) 874-1384
Toll Free:
1-877-874-9343
www.ccaemployerlaw.com

EXPERTISE • EXPERIENCE • EXCEPTIONAL SERVICE

"The Employers' Choice"

7 Steps to PIPEDA Compliance

1 Become familiar with PIPEDA's provisions, with particular attention to the definition of personal information and the ten privacy principles in the Schedule to the legislation.

2 Designate a privacy officer (or team) who will be responsible for the organization's compliance.

3 Identify the general purposes for the collection of personal information by the organization. This exercise will assist the assessment of what personal information is required by the organization in order to conduct its business.

4 Audit existing personal information holdings. PIPEDA does not permit the "grandfathering" of personal information collected prior to January 1, 2004 and, accordingly, such information could be regulated with respect to further use and disclosure.

5 Identify the "gaps" that exist between current practices and compliant practices, and address gaps by developing and implementing compliant practices.

6 Develop a privacy policy that sets out how the organization handles personal information, and that communicates access and complaints procedures. The privacy policy should address the ten principles set out in the Schedule to PIPEDA.

7 Communicate the compliance strategy. The privacy policy and compliance plan should be communicated to all personnel within the organization.

Obligations Imposed

In addition to the requirements discussed above, PIPEDA requires organizations to implement other measures to ensure the protection of personal information in their possession and/or control. Such measures include the following:

- Designating an individual (or team), who will be accountable for ensuring that the organization complies with PIPEDA.
- Identifying the purposes for the collection of personal information before or at the time the information is collected.
- Ensuring that personal information is collected by fair and lawful means, and that collection, use and disclosure of the information is limited to and consistent with the purposes identified.
- Ensuring that all personal information is secure and accurate, and is retained only as long as is necessary for the fulfillment of the identified purposes, except as required by law (such as retention requirements under the *Income Tax Act*).
- Allowing individuals access to their personal information which is possessed by the organization, subject to limited exemptions.
- Implementing a privacy policy that describes the organization's privacy practices, and that communicates how individuals can obtain access to their personal information.
- Providing internal processes to allow individuals to raise challenges to the organization's compliance with PIPEDA (i.e. an internal complaints process).

Consequences of Non-Compliance

The enforcement provisions of PIPEDA are triggered when an individual files a complaint about an organization's personal information handling practices. The Privacy Commissioner of Canada ("Commissioner") may also initiate a complaint if the Commissioner is satisfied that there are reasonable grounds to believe that an organization is not in compliance with the legislation. Once a complaint has been filed, the Commissioner's office conducts an investigation and may attempt to resolve the matter through mediation or conciliation. The Commissioner may issue recommendations to the organization advising how it should improve its privacy practices. If the organization does not follow the recommendations, the Commissioner may apply to the Federal Court for a hearing, and the Court may order the organization to correct its practices and/or award damages to the complainant. In addition, certain contraventions of PIPEDA could result in the imposition of fines to a maximum of $100,000.

Although PIPEDA is now in force in Ontario, given its complaints-based enforcement structure, organizations that have not commenced or completed their privacy compliance initiatives should still take the time to ensure that they do so in a thorough and effective manner. There are a number of resources available to assist your organization's privacy compliance efforts, including our firm's professional Privacy Law services that include:

- assisting with privacy audits and gap assessments;
- developing privacy policies and compliant practices;
- drafting disclosure agreements for third parties that require them to meet privacy compliance obligations;
- conducting training and education on organization compliance obligations; and
- providing advice and representation with respect to responding to complaints and enforcement proceedings.

We invite you to visit our website at www.ccaemployerlaw.com for more information on PIPEDA and the services we provide, or to access our risk assessment checklist that we have designed to assist organizations in evaluating their current personal information handling practices.