By Katherine E. Ford

Privacy and the workplace

The importance of managing employees' personal information

In the wake of recent changes to Canada's privacy law, many employers struggle to understand their legal obligations to protect the personal information of employees, as well as what steps need to be taken to safeguard this information.

However, it's vital that employers understand why protecting personal information is so important and have a plan to protect the privacy of personal information collected in the workplace.

This article should provide managers the facts you need to get started.

What is PIPEDA?

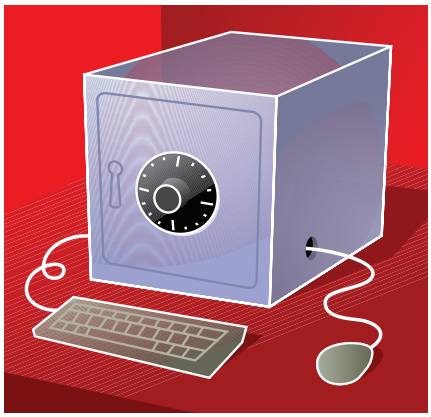
On January 1, 2001, the federal government enacted the *Personal Information Protection and Electronic Documents Act* (*"PIPEDA"*).

As a result, all federally-regulated, private sector organizations were required to comply with its provisions as of January 1, 2001. The provinces were given until January 1, 2004 to either enact legislation that was "substantially similar" to *PIPEDA*, or to comply with *PIPEDA*. British Columbia, Alberta and Quebec enacted "substantially similar" legislation. To date, the remaining provinces have not. As such, *PIPEDA* applies to the private sector of all remaining provinces.

In Ontario, *PIPEDA* applies to any "organization" (an intentionally broad term) that collects, uses or discloses personal information in the course of commercial activities.

Does PIPEDA govern employee information?

PIPEDA seeks to protect "personal information" which includes *any* information that is about an identifiable individual. Examples of "personal information" include one's age, home phone number, birth date, social insurance number, income, medical records, disciplinary records, credit records and opinions, evaluations or comments relating to a specific individual. Significantly, *PIPEDA* does not apply to *employee* personal information, unless an organization is federally-regulated (i.e. banks, airlines, telecommunications) or uses the personal information for a commercial purpose. So, while *PIPEDA* sets out the statutory obligations for customer information held by an Ontario organization, *PIPEDA may not* apply to its employee personal information.



Four reasons why organizations should extend PIPEDA to employee information

Despite this, there are good business reasons why employers should adopt practices for handling the privacy of employee information.

One policy works best

First, for employers with multi-jurisdictional operations, it's more efficient (and sometimes even cheaper) to have one consistent approach to the handling and safeguarding of employee information across all offices, including in those provinces (such as British Columbia, Alberta and Quebec) where statutory privacy obligations relating to employee personal information already exist.

It increases the likelihood of compliance

Second, since employees typically play a significant role in effectively carrying out an organization's *PIPEDA* obligations, it's in each employer's best interest to have employees "buy in" to the importance of adhering to privacy laws. "Buy in" is less likely to occur where an organization only adopts information management practices for its customers' personal information but not its employees' personal information.

Be prepared

Third, it is expected that other jurisdictions, like Ontario, will ultimately introduce privacy laws that will include the requirement for employers to protect employee personal information. Consequently, organizations already treating both customer and employee personal information to legislative standards will be prepared.

It's good business

Finally, having sound privacy practices enhances an organization's public image and reputation. Customers and employees feel assured that their personal information is being kept confidential. For this reason, compliance with privacy legislation makes good business sense.

The 10 principles of PIPEDA

Under *PIPEDA,* an organization's obligations are based on 10 principles. Together, these principles are designed to limit the circumstances, and to provide individuals with some degree of control over the manner in which their personal information is collected, used and disclosed. While there are several components and exceptions associated with each principle, the following is a brief outline of an organization's obligations:

1. **Accountability:** Each organization must appoint a "chief privacy officer" ("CPO"), or other designated individual, whose mandate is to ensure the organization's compliance with the legislation and train staff on the organization's policies. If a customer or employee calls asking for a copy of the organization's privacy policy or has questions about the organization's practices, the CPO must be able to provide the information.

2. **Identifying purposes:** *PIPEDA* requires organizations clarify the purpose for which personal information is collected. Prior to or at the point of collection, individuals should be informed of the specific purpose for which information is being collected. Broadly worded catch-all phrases that identify the reasons for collection (i.e. "for employment purposes") are not acceptable. Be specific.

3. **Consent:** Individuals must give consent to the collection, use and disclosure of personal information by an organiza-

tion. This consent must be *meaningful*, in that an individual must be able to reasonably understand how their information will be used or disclosed. Where information is of a sensitive nature (e.g. medical or financial information), express consent will be necessary. An "opt-out" form of consent (i.e. assuming an individual consents unless they indicate otherwise) is rarely acceptable.

4. Limiting collection: *PIPEDA* limits collection to only that information that is required for the identified purpose. So, for example, collecting more information than is necessary – in order "to be sure you have enough information" – is inconsistent with the law. The legislation also requires that collection be undertaken through "fair and lawful means", such that individuals are not deliberately deceived or misled about the purpose for which the information is being collected.

5. Limiting use, disclosure and retention: An organization is required to use and disclose information only for the purpose it was collected. Where an organization wishes to use previously acquired information for a new purpose, fresh consent for that new use must be obtained. For example, one employer landed in hot water when it obtained consent to collect its employees' SIN number for payroll purposes and subsequently used the numbers for reasons unrelated to the original purpose (in this case, to use it as an internal password).

Furthermore, personal information should be kept only as long as reasonably necessary to satisfy the purpose for which it was collected. Organizations are required to create guidelines for the retention and destruction of personal information once it is no longer necessary. Many employers breach *PIPEDA* by either keeping employee information on file for longer than required (i.e. unreviewed resumés). Employers should destroy unsolicited resumés immediately. Alternatively, employers can run afoul of *PIPEDA* by retaining information for too short a period. Where a complaint or access request has been made, the personal information at issue must be retained until such time as the individual has been able to exhaust any possible recourse under the legislation.

6. Accuracy: Personal information must be kept as accurate, complete and up-to-date as necessary for the identified purpose.

7. Safeguards: Organizations are required to deploy technological, physical and organizational security safeguards to protect personal information within their care. These safeguards should protect against loss or theft of personal information, as well as unauthorized access, use or disclosure. The degree of security required will vary depending on the sensitivity of information, with more sensitive information being afforded a higher level of protection.

8. Openness: *PIPEDA* requires that organizations make information about their privacy practices and policies easily available. This includes an explanation of the process through which an individual can gain access to personal information about him or herself or lodge a complaint, and inquire about the type of personal information collected by the organization.

9. Individual access: An employee whose personal information is held by an organization should, upon request, be informed of the existence, use and disclosure of the personal information. The individual should also be able to access that information on request within 30 days, be able to challenge its accuracy and completeness, and have it amended, where appropriate. Any inaccurate information must be corrected.

10. Challenging compliance: Organizations must implement an accessible complaint procedure, acknowledge receipt of any complaint in a timely manner, and investigate all complaints received.

How do I become compliant?

The amount of work required to become compliant will depend on an organization's size, complexity of operations and existing practices. We generally recommend a "five step" plan to privacy compliance:

- Develop a privacy team.
- Perform an audit on your organization's existing practices.
- Analyze the gaps between *PIPEDA*'s requirements and your existing practice.
- Implement an action plan to "fill in the gaps" and bring your organization in line with *PIPEDA*.
- Monitor and assess your organization's ongoing compliance. ❍

Katherine E. Ford is a lawyer with the employment and labour law firm Sherrard Kuzz LLP in Toronto. The firm specializes in advising and representing management in all matters of employment and labour law including recognized expertise in Privacy Compliance.. Katherine can be reached at 416-603-0700, 416-420-0738 (24 Hour) or by visiting www.sherrardkuzz.com.