
Ensuring compliance with the *Personal Information Protection and Electronic Documents Act*: what your organization should do

In the last issue of *FOCUS*, we discussed the main outlines of the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*, which came into force January 1, 2001. (See "[The Personal Information Protection and Electronic Documents Act: What it means for federally regulated businesses and their employees](#)"). As of that date, federally regulated businesses are required to comply with the Act, both in respect of their customers and their employees.

As we saw in the last issue, the new Act imposes obligations with respect to the collection, use, retention and disclosure of personal information about employees' personal information. As well, the federal Privacy Commissioner is given new investigative and oversight powers and employees are given new rights, specifically with regard to the right to have personal information collected, used or disclosed only with their knowledge and consent, and the right to access their personal information. Moreover, employees can enforce their rights by way of a complaint to the Privacy Commissioner and, in some instances an action in the Federal Court.

Successful compliance is best achieved through the establishment of a corporate privacy policy. In this article, we will look at the sorts of issues employers should bear in mind when crafting a privacy policy.

The key elements that the policy should include are:

- a general statement of the policy's purpose and principles
- designation of a person as privacy co-ordinator and a description of that person's role
- identification in general terms of the purpose for which personal information is collected
- mechanisms for obtaining consent
- limits on the use, disclosure and retention of personal information, including a time limit for retention
- mechanisms to ensure the security of information
- procedures to structure employees' right of access to the information
- procedures for challenging the employer's compliance with its privacy obligations

GENERAL STATEMENT

To inform employees of the purpose of the policy, it may be useful to produce a statement of why the policy is being adopted and the principles underlying it. This could entail a description of *PIPEDA*, a statement that the employer is committed to meeting its privacy

obligations, and how the policy will ensure compliance with the new legislation.

Such a summary statement might indicate that personal information may only be collected if it relates specifically, and is reasonably necessary to, the organization's business activities, and if the individual to whom the information relates consents to the collection.

PRIVACY CO-ORDINATOR

The first principle of the CSA Model Code for the Protection of Personal Information rules, which are incorporated into *PIPEDA*, is accountability. In this context, accountability means that the person or persons responsible for ensuring compliance must be clearly designated. Given the importance of the role, the privacy manager or co-ordinator should be someone drawn from senior management.

As the key responsibility here is ensuring compliance, this person will oversee the organization's information collection, retention, use and disclosure activities. He or she will also be responsible for how the business deals with complaints or access requests.

PURPOSE FOR COLLECTING INFORMATION

The policy should specify that employees are to be told the purpose for which personal information is being collected before or at the time the collection occurs. The purposes must be reasonable in the sense that they must be what a reasonable person would expect in the circumstances. In general, it is prudent to steer a middle course between overly broad purposes, which may be unreasonable, and excessively specific purposes, which may require new consents for any added purposes. Employees responsible for collecting information should be able to explain the purpose if asked.

CONSENT

Consent is required for the collection, use or disclosure of personal information. The policy should provide for consent statements to be included in certain documents, such as job application forms and performance reviews. Consent statements should be framed in terms of the purposes for which the information is being collected or will be used. If the information is to be used for a purpose other than that set out originally, the policy should provide that a new consent should be obtained.

The policy should indicate the circumstances in which consent is not required, such as the investigation of a breach of a contract or contravention of the law. In some cases, implicit consent is sufficient, such as in emergencies, or where collection is clearly in the interest of the individual and consent cannot be obtained in a timely way. However, in others, for example where the information is sensitive, consent must be explicit.

Further, while employees have the right to withhold consent, the employer may, in appropriate circumstances, be entitled to deny continued employment for failure to provide consent. Some thought should be given to when consent is indispensable. In such cases, employees should be clearly informed of the consequences of failure to provide consent.

The knowledge and consent obligations under *PIPEDA* likely apply to various forms of employee monitoring. Therefore, where monitoring is contemplated, the policy should provide for how consent is to be obtained in respect of the monitoring activity.

LIMITS ON RETENTION

An important component of any privacy policy is that relating to the disposal of information. Consideration should be given to the appropriate retention periods for different types of personal information. Generally, information should be retained only as long as necessary to fulfil the purpose for which it was collected. Schedules should be established to destroy, erase, or make anonymous personal information which is no longer required.

SAFEGUARDING INFORMATION

The policy should ensure that mechanisms and procedures are in place to keep personal information secure and confidential. The following are the types of measures that should be considered:

- keeping personal information in locked file cabinets
- restricting access to electronic personal information
- requiring all employees to sign confidentiality agreements in respect of personal information
- establishing security measures in respect of the destruction of personal information
- establishing procedures for transmitting personal information to ensure that the security of the method of transmission is appropriate to the sensitivity of the information
- making employees aware of the importance of keeping personal information confidential. (For example, advising employees to avoid leaving personal information unattended when displayed on computer screens or in hard copy form.)

RIGHT OF ACCESS

Individuals must be given the right to access their personal information and to have it amended as appropriate. The policy should specify the procedure for allowing access. For example, it could provide that access will be granted at reasonable intervals within a given time and that a designated individual will be present while the employee views his or her file.

With respect to requests to amend the information, the policy should indicate a willingness to amend information where the information is found to be inaccurate or incomplete. Where the organization does not agree that an amendment is required, the policy should provide that the employee will be allowed to attach a notation to the file.

The policy should also stipulate the conditions under which access will not be granted. These include where access would reveal information that

- is personal information about a third party,
- may harm another person,
- is the subject of litigation, or
- could harm the organization's competitive position.

However, where the information can be severed so as to permit access without creating one of the above conditions, the organization is obliged to do so.

COMPLAINT MECHANISM

PIPEDA obliges the organization to allow employees and customers to challenge its personal information practices, and to respond to all inquiries and complaints. The policy should set out the procedure for making complaints, the components of which could include

- the individual to whom complaints should be addressed,
- the time frame within which a response will be provided,
- appeal procedures, including the right to go directly to the federal Privacy Commissioner, and
- the person responsible for investigating the complaint or responding to inquiries.

In Our View

Employers subject to *PIPEDA* will have to be sensitive to the requirements of employee knowledge, consent, and access. They will also have to be alert to safeguard the personal information under their control. Clearly, a policy along the lines of that described in this article will go some way to getting an organization up to speed in meeting these new obligations. Lawyers at our firm are ready to provide assistance in crafting policies and protocols that fit the needs of your organization. (For more information on privacy legislation, please see "[Ontario releases draft privacy legislation](#)".)

For further information, please contact [Colleen Dunlop](#) at (613) 563-7600, Extension 222, or [Steven P. Williams](#) at (613) 563-7660, Extension 242.

For more news about recent developments in Employment and Labour Law, and for information about how our firm can assist you, please visit <http://www.emondharnden.com/>