PRIVACY TRAINING

Posted on June 28, 2015

Categories: Insights, Publications

Data collected in jurisdictions with mandatory breach reporting indicates that the most common cause of privacy breaches is human error. Such mistakes include inappropriate document disposal, loss of unencrypted portable data storage devices, sharing/disclosing passwords, misdirected faxes, and allowing all email addresses to be viewable in mass emails.

Privacy training can avoid these types of errors by ensuring that employees understand their obligations under applicable laws and policies, as well as how these laws and policies apply to their every day activities.

In addition to being good practice, to avoid privacy breaches, privacy training is required by law in Canada. Article 4.1.4 of the *Personal Information Protection and Electronic Documents Act* states that: "Organizations **shall** implement policies and practices to give effect to the principles, including... **training** staff and communicating to staff information about the organization's privacy policies and practices..." (emphasis added). In addition, case law and guidelines published by provincial privacy commissioners are clear that training is implicitly required pursuant to accountability and security provisions in substantially similar provincial privacy legislation.

Therefore, organizations should implement training programs that include: (1) general privacy training for all new employees; (2) role specific training for relevant employee groups; and (3) regular training updates.

General training for all employees

Training should be mandatory for all new employees before they access personal information. This general training should, at a minimum:

- Ensure that employees are aware that laws apply to collection, use, storage and disclosure of personal information, and failure to comply with such laws can have consequences both for the individual and the organization;
- Include an overview of consent requirements under applicable laws, including how to obtain consent, as well as when consent can be implied and how it can be withdrawn;
- Provide an overview of the purposes for which the organization collects, uses and discloses personal information, so that employees can communicate this information to customers and other third parties;

- Provide information respecting the organization's privacy policies, including where to find those policies and how to direct customers to the policies;Provide guidelines for portable media devices (e.g., minimize their use, ensure they are kept secure, require encryption);
- Review guidelines for acceptable passwords and discuss restrictions on sharing of passwords;
- Provide guidelines for faxing and emailing personal information;
- Review appropriate document disposal methods (e.g., documents containing personal information should be shredded and not placed in unsecured trash receptacles);
- Instruct employees on how to recognize and respond to privacy inquiries, complaints and access requests, including how and when to elevate such matters to the person(s) within the organization who are responsible for privacy compliance; and
- Instruct employees on how and when to report actual or suspected privacy breaches/incidents.

In general, all employees should be able to recognize privacy issues and understand who they can and should contact for support when such issues arise.

Role specific training

Training employees on broad, general legal principles is not an effective strategy for helping them recognize and deal with privacy issues that arise in the course of their day-to-day functions. It is far more effective to provide targeted, role-specific privacy training to relevant employee groups. For example:

1. ***Human Resources*** – HR employees need to understand the different legal requirements that apply to collection, use and disclosure of employee personal information as opposed to customer information. Training for HR staff should also address privacy issues that relate to recruitment (e.g., employment applications, interviews, background checks), employee monitoring (e.g., computer, phone, video, GPS), outsourcing (e.g., payroll, benefits), and sensitive information such as employee medical data. HR staff will also need to understand the appropriate disciplinary response when an employee is found responsible for breaches of the organization's privacy policy.
2. ***Information Technology*** – Security will be a main focus of training for IT staff, including the role of such persons when a data breach occurs. IT staff will also need to understand statutory requirements to implement technological security measures appropriate to the sensitivity of information, so that they can assist the organization to comply with such legal obligations. Of course, IT staff also need to understand restrictions on accessing and altering personal information without a legitimate business purpose, since such employees are often able to access a broad range of personal information contained on the organization's systems. Finally, IT staff should understand limits on record retention (e.g., restrictions upon retaining personal information after it is no longer necessary and/or consent is revoked), since such

employees may design or administer aspects of the organization's system that determine how long information is retained before it is archived and/or permanently deleted.

3. ***Marketing*** – Training for marketing employees should address consent requirements applicable to using personal information for secondary marketing purposes, including the requirement for fresh consent to use such information for new purposes. Marketing employees should also be provided with information on legal developments applicable to their function, such as recent cases on online behavioural advertising and Canada's new anti-spam legislation. Marketing employees also need to understand when they need to seek guidance or approval from the organization's Chief Privacy Officer or legal counsel.

These are just a few examples of role specific training. Organizations should take the time to identify employee groups that may require training within their specific business, and develop custom training sessions applicable to each relevant function.

Training updates

Privacy law is rapidly developing in Canada and worldwide. Furthermore, organizations are rarely static, and the way that they collect, use and disclose personal information changes periodically. Employees should receive training on any new requirements or restrictions arising out of legal, organizational or policy changes. Training updates should also include a refresher on important basics, so that employees remain cognizant of their core obligations throughout their employment.

by Lyndsay A. Wasser

A Cautionary Note