



Canadian Privacy 101: Employers Be Aware!

Insights
12.30.15

This is the first post in a three-part series.

If you work for a U.S.-based company with Canadian operations, your organization probably understands its obligations to comply with Canadian employment and tax laws. But is your company up to date on the protection of privacy and protection of personal information under Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)? Moreover, many provinces have their own legislation governing data privacy and protection that accompanies PIPEDA. Although prudent employers should be aware of data privacy and protection laws in each of the provinces in which they do business, the good news is that PIPEDA does not apply to a company which operates wholly within a province that has legislation deemed substantially similar to the PIPEDA, unless the personal information crosses provincial or national borders. For example, Alberta, British Columbia and Quebec have general private-sector legislation that has been deemed substantially similar, and therefore PIPEDA would not apply.

The Personal Information Protection and Electronic Documents Act

PIPEDA, enacted in 2001, generally governs how private-sector organizations, engaged in commercial activities, collect, use or disclose personal information in the course of doing business throughout Canada. PIPEDA is enforced by the Office of the Privacy Commissioner of Canada, which maintains a website including helpful guidance for companies subjected to its requirements.

An Employer's responsibilities under PIPEDA

PIPEDA requires that a company must obtain an individual's consent when it collects, uses or discloses an individual's personal information in the course of a commercial activity. This includes employment activities. In an employment setting, an employee has the right to know what information is held by the company and to dispute any inaccuracies. Companies may only use the personal information for the purpose it was collected, and must ensure the personal information is protected by appropriate safeguards. Although PIPEDA protects much information related to employees, including information regarding employee age, ethnic origin, evaluations, disciplinary action, employee files and credit records, other information, such as business contact information, including employee name, title, business address, telephone number and e-mail address are exempted.

Under PIPEDA, companies are expected to abide by the Ten Principles of Fair Information Practices. In general, this means that employers are required to have a system of compliance in place to ensure that PIPEDA's requirements are met, including developing a formal compliance program, appointing a compliance manager, and protecting all personal information. The company's compliance program should address the purpose for collecting personal information. Namely, will the information be used for a legitimate purpose and is it reasonably necessary to collect such information?

Once the company has determined the information to be collected, it must obtain informed consent from the employee, specifying what information will be collected, how it will be used and whether it will be disclosed. Any such explanation should be clear and straightforward, and employers should keep a written record of any such consent. Collection, use, disclosure and retention of personal employee information should be limited to the use disclosed, and kept only as long as necessary to serve the purpose for which it was collected. Employers have a responsibility to safeguard the information they collect and to ensure that the information is accurate. Finally, employers should be open about their privacy practices and provide easy access to the employee's personal information upon the employee's request. Companies must provide a clear path to make complaints should the policies be violated or an employee has concerns.

The Office of the Privacy Commissioner of Canada oversees compliance with PIPEDA.

Employees may complain to the Privacy Commissioner if they believe their rights under PIPEDA have been violated. The Privacy Commissioner has the authority to investigate any such complaints, and the time in which to complain is not specified (although the Privacy Commissioner may decline to investigate any complaints it believes were not filed within a reasonable time frame). Complaints alleging that access to personal information was denied must be filed within six months of the alleged denial.

In most cases, the Privacy Commissioner will work with the parties to negotiate a resolution of the complaint. Where the Privacy Commissioner has reason to believe the Company's practices are not compliant, the Privacy Commissioner can initiate an audit of the employer's compliance with PIPEDA. Additionally, under certain circumstances, the Privacy Commissioner or the complainant may apply for a hearing to the Federal Court. Although the Privacy Commissioner has the authority to compel the production of witnesses or evidence, it generally will not do so where there is voluntary cooperation.

Related People





Danielle S. Urban, CIPP/E

Partner

303.218.3650

Email