Manitoba's New Privacy Law Has Implications For Cross-Border Employers

Insights
11.01.13

Last month, the Canadian Province of Manitoba enacted privacy legislation governing the collection, use and dissemination of personal information, including employee personal information. With the legislation, Manitoba joins the other Canadian Provinces of Quebec, Alberta, and British Columbia in providing special protection for employee personal data. Private-sector employers with operations in Manitoba should ensure their data collection and protection are in compliance with the Manitoba Personal Information Protection and Identity Theft Protection Act ("PIPITPA"), or risk fines of up to $100,000.

Employers are Responsible for Personal Information in their Custody or Control.
Under PIPITPA, an organization must take care to ensure that "personal information," defined as information about an identifiable individual, in its custody or under its control, may only be collected, used or disclosed with the permission of that individual. This includes personal information related to employees. To that end, employers should designate a compliance officer to oversee the collection, use and dissemination of personal data, and must establish policies and procedures governing the employer's handling of employee personal data.

In general, the PIPITPA employs a consent-based model, and individuals will be permitted to provide limited consent or withdraw previously-granted consent for the collection of personal data. There are carve-outs for "personal employee information" in that consent is not required where the use or disclosure of the personal information is used to recruit new employees or is regarding an employee of the employer. To come within this exception, however, employers must ensure that the collection, use or disclosure is reasonable for its purposes and the information relates solely to the employment relationship. Current employees must still be provided notice and reason for the collection, use, or disclosure of personal data.

Under PIPITPA, "employee" is defined broadly to include volunteers, students and apprentices, among others.

Breach and Corrections
In the event an employee's personal data is compromised through theft, loss, or misuse, the employer must notify its employee of the breach as soon as is reasonably practical, provided that the employer has reason to believe that the compromised data would be unlawfully used. Employees will be able to claim damages arising out of any such breach. Employers with policies and

procedures addressing PIPITPA will have a due diligence defense available to them in event of a breach, however. There does not appear to be a specific complaint mechanism under PIPITPA, although there is a private right of action, and privacy breach class actions will be permitted.

PIPITPA also establishes the individual's right to review his or her information and make corrections where necessary, although there is no absolute right of the individual to demand corrections where the organization has reasonable grounds to believe a correction is not warranted. Where the employer declines to correct personal information, the employee record must nevertheless be annotated with an explanation that a correction was requested but denied.

PIPITPA is still awaiting proclamation, which sets the date the legislation will come into force. Although no effective date has been set yet, employers are advised to begin planning for PIPITA as soon as possible.

Related People

Danielle S. Urban, CIPP/E
Partner
303.218.3650
Email