Employee Data Privacy – Canada

Breach Notification

Are there any data breach notification requirements?

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Local data protection regulations have required data controllers to report such breaches in certain circumstances. In Canada, breach notification requirements can vary by province and by those subject to the Federal Personal Information Protection and Electronic Documents Act (PIPEDA).

Alberta

In Alberta, organizations are required to notify the Alberta Information and Privacy Commissioner of any incident involving loss, unauthorized access or disclosure of personal information where there is a real risk of significant harm to an individual as a result of the breach. Notice to the Information and Privacy Commissioner must be written and include:

- a description of the circumstances of the loss, unauthorized access or disclosure;
- the date or time period during which the incident occurred;
- a description of personal information involved;
- an assessment of the risk of harm to individuals;
- an estimate of the number of individuals to whom there is a real risk of significant harm;
- a description of all steps the organization has taken to reduce the risk of harm to individuals;
- a description of all steps the organization has taken to notify individuals; and,
- the name of and contact information of a person who can answer the Commissioner's questions about the incident, on behalf of the employer.

Alberta's Information and Privacy Commissioner has the authority to require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss, unauthorized access or disclosure. When required, the notice generally should be given directly to the impacted individuals and include:

- a description of the circumstances of the incident;
- the date or time period during which the incident occurred;
- a description of the personal information involved;
- a description of all steps the organization has taken to reduce the risk of harm; and,
- the contact information of a person who can answer questions about the incident, on behalf of the employer.

British Columbia

British Columbia (BC) does not currently have a data breach notification law, but the BC Information and Privacy Commissioner suggests that notification may be appropriate in certain circumstances, upon an assessment by the organization of the severity of the breach.

Quebec

The Quebec Commission d'accès à l'information (CAI) has issued guidelines on what businesses should do in the event of a security breach, and when they should notify individuals. The CAI also recommends that organizations complete a voluntary incident declaration form (available on the Quebec CAI website).

Effective September 2022, part of Quebec's "Act to Modernize Legislative Provisions Respecting the Protection of Personal Information" (Law 25) will go into effect, including the requirement for companies to report incidents to the CAI and to individuals whose personal information was affected by an incident which presents a "risk of serious harm." When assessing risk, companies must consider "the sensitivity of the information concerned, the anticipated consequences of its use and the likelihood that such information will be used for injurious purposes."

In addition, organizations must take reasonable measures to reduce the risk of harm resulting from the use of information and to prevent the recurrence of incidents. Companies will also be required to keep an incident register.

PIPEDA

Effective November 1, 2018, organizations that are subject to the Federal Personal Information Protection and Electronic Documents Act (PIPEDA) must report any breach of security safeguards to the Privacy Commissioner if the breach involved personal information under the organization's control and it is reasonable (given the circumstances) to believe that the breach creates a real risk of significant harm to an individual. The report must be written and provided to the Commissioner as soon as feasible. It should include:

- a description of the circumstances of the breach and the cause (if known);
- the day or period the breach occurred (or, approximate period);
- a description of the personal information that was the subject of the breach (to the extent known);
- the number of individuals affected (or approximate number);
- a description of steps the organization has taken to reduce the risk of harm or mitigate harm to individuals;
- a description of steps the organization has taken or plans to take to notify affected individuals; and,
- the name of and contact information of a person who can answer the Commissioner's questions about the incident, on behalf of the employer.

Unless prohibited by law, employers shall notify an individual of any breach involving the

individual's personal information under the employer's control if it is reasonable to believe that the breach creates a real risk of significant harm to the individual. The notice must be written and provided to the individual as soon as possible. The notice should include:

- a description of the circumstances of the breach;
- the day or period during which the breach occurred (or approximate period);
- a description of the personal information that is the subject of the breach (to the extent known);
- a description of steps the employer has taken to reduce the risk of harm;
- a description of steps that individuals can take to reduce the risk of harm or mitigate harm; and,
- the contact information that the affected individual can use to obtain further information.

When determining whether a breach created a real risk of harm, employers should consider the sensitivity of the personal information involved and the probability the information has been or will be misused.

In the event the employer notifies individuals of a breach, the employer must also notify any organization, government institution or part of a government institution that it believes can reduce the risk of harm or mitigate harm.

Employers who are subject to PIPEDA must create and maintain a record of the breach for 24 months and allow the Office of the Privacy Commissioner to access those records upon request (note: this record must be completed even when there is no risk of harm to individuals).

Last updated July 2022.