QUICK-REFERENCE

Mandatory reporting for privacy incidents

Objective

Explain reporting requirements for businesses when a breach of security safeguards occurs

On November 1, 2018, the *Breach of Security Safeguards Regulations* came into force. The regulations require that businesses subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) report any breach of security safeguards and keep a record of all breaches.

Under these new requirements, PIPEDA requires organizations to notify individuals affected by the breach if there is a *real risk of significant harm.* Any time you discover that a breach poses a real risk of significant harm, it must be reported, even if only one person is affected. The factors used to determine if a security breach is a real risk of significant harm include the sensitivity of the personal information involved in the breach and how likely it is that this personal information has been, is being, or will be misused. If these criteria are met, the incident must be reported to the Office of the Privacy Commissioner of Canada.

Target audience: Organizations subject to PIPEDA that “manage” the personal information involved in a breach.

Personal Information (PI)

Personal information is any information about an identifiable individual, or any information that can be used to identify an individual when used alone or combined with any other information.

Breaches of security safeguards involving personal information

A breach of security safeguards occurs when personal information is lost, disclosed or accessed without authorization. This situation can occur when the organization’s security safeguards have been breached, or if the organization has failed to set up appropriate safeguards.

What you need to know about your requirements under the regulations

- These obligations apply to both small and large businesses.
- Fines may be imposed on any organization that knowingly contravenes PIPEDA's reporting, notification and recordkeeping requirements related to breaches of security safeguards.
- There must be a record kept of every breach of security safeguards, whether there is a real risk of serious harm or not. These records must comply with PIPEDA requirements.
- The law requires businesses to keep records for two years. There may be other legal requirements that require you to keep them for longer.
- The Office of the Privacy Commissioner has issued guidelines on what to include in a report and how to file reports. You can find the details on their website.
- Unless otherwise prohibited by law, each time that you determine that a breach of security safeguards poses a real risk of serious harm to an individual, you must notify the individuals involved. The notification must be clear and obvious, and given directly to the individual, except in certain circumstances described in the regulations.
- The law requires that individuals be notified as soon as possible after you have determined that a breach has occurred posing a real risk of serious harm.
- The notification must include the following information, as specified in the regulations:
    - the circumstances of the breach
    - the date or period in which the breach occurred, or the approximate period if the exact period is unknown
    - a description of the personal information that is the subject of the breach, to the extent that it is known
    - the steps that you've taken to reduce the risk of harm that could result from the breach
    - the steps the affected individuals could take to reduce or mitigate the risk of harm that could result from the breach
    - contact information that the individual could use to get more information about the breach
- If you determine that the individuals must be notified of the security breach, because it poses a real risk of significant harm, you must also notify any other government institutions or organizations that you believe could also reduce or mitigate the harm that could result from this risk.

Protection of Personal nformation Best practices

- Double-check the recipients of all emails, faxes and letters.
- Use blind carbon copy (bcc) when sending out mass emails.
- Don't leave documents containing personal information unattended.
- Lock your workstation when you leave, even for short absences.
- Don't leave documents containing personal information on your desk.
- When speaking to someone over the phone, confirm their identity and make sure you have their consent before disclosing personal information by phone.
- Make sure that your organization has compliant practices for disclosing personal information.

For more information, the Office of the Privacy Commissioner has published an article, *Respond to a Privacy Breach at Your Business*. You can read it here.