BRITISH COLUMBIA'S PRIVACY REGULATOR ISSUES NEW PRIVACY BREACH GUIDANCE: HERE'S WHAT YOU NEED TO KNOW

Posted on February 16, 2023

Categories: Insights, Publications

The Office of the Information and Privacy Commissioner for British Columbia ("**BC OIPC**") recently released guidance setting out its recommendations for private organizations in British Columbia that experience a privacy breach (the "**Guidance Document**"). The BC OIPC's release of recommendations in this regard is a notable development given that British Columbia is currently the only Canadian jurisdiction that does not have statutory breach reporting or notification requirements.

Guidance Document

In the Guidance Document, the BC OIPC regards any unauthorized access to or collection, use, disclosure, or disposal of personal information as a privacy breach. The BC OIPC considers activities to be "unauthorized" if they occur in contravention of British Columbia's *Personal Information Protection Act* ("**BC PIPA**"). Examples of privacy breaches include the inadvertent sharing of personal information with the wrong person and theft of personal information under an organization's control.

The Guidance Document outlines four key steps that organizations should take when responding to a privacy breach: (1) contain the breach; (2) evaluate the risks; (3) consider notifying affected individuals and other third parties; and (4) take appropriate go-forward preventative measures.

Step 1: Containing the Breach

Effectively containing a privacy breach will depend, in part, on how the breach occurred. For example, where a breach involves the unauthorized access to an organizations computer network, appropriate containment measures could include changing computer access codes, shutting down the server that was breached and adding additional digital or physical protective measures.

The BC OIPC also recommends that the organization promptly activate their breach management policy and take care not to destroy evidence that may be useful in identifying the cause of the incident. If an organization does not have a breach management policy in place, the BC OIPC recommends taking the following steps:

1. appoint an individual to spearhead the initial investigation;
2. inform the organization's privacy officer and/or the person responsible for security as well as any other members who should know about the breach;
3. determine whether a breach response team must be created; and
4. if the breach involves criminal activity, notify law enforcement.

While not set out in the Guidance Document, it is important to engage external counsel early in the process to obtain advice on applicable legal and regulatory requirements in response to the breach and to otherwise manage associated legal risks.

Step 2: Evaluating the Risks

The Guidance Document recommends that organizations consider the following factors to evaluate the risks arising from a privacy breach:

1. the personal information involved, including the sensitivity of such information and the potential for misuse;
2. the cause and extent of the privacy breach, including the nature of the incident, continuing vulnerabilities, and whether compromised date was encrypted or otherwise not readily accessible;
3. the individuals or others affected by the breach, including the number of such individuals and the organizations relationship to them; and
4. the foreseeable harm to affected individuals, the public, and the organization itself that may arise from the breach.

Step 3: Notifying Third Parties

The Guidance Document encourages organizations to consider whether notification to affected individuals and other third parties may be appropriate in the circumstances. Notably, BC PIPA does not currently require private organizations to notify affected individuals or the BC OIPC when a privacy breach has occurred. As such, the decision to do so is voluntary. As noted above, it is important to seek legal advice to develop a breach response strategy that is appropriate in the circumstances.

The Guidance Document recommends consideration of the following factors to determine whether notification to affected parties is appropriate:

1. whether legislation or contractual obligations require notification;
2. whether there is a risk of identity theft, fraud, physical harm, or damage to reputation; and
3. whether there is a risk of loss of business or employment opportunities or loss of confidence in the

organization.

If an organization determines that notification is appropriate, the Guidance Document recommends doing so as soon as possible unless notification would impede an ongoing criminal investigation. The Guidance Document recommends that such notification be made directly to affected individuals and include: (i) the name of the organization; (ii) the date the organization was made aware of the breach; (iii) a description of the breach and potential harms; (iv) a description of the personal information involved; (v) the steps taken to control or reduce potential harms; (vi) steps the individual can take to further mitigate the risk of harm; (vii) contact information for an individual within the organization who can answer questions or provide further information; and (viii) a statement that the organization has notified the BC OIPC (if applicable).

The Guidance Document also encourages organizations to consider whether to inform other third parties or authorities of the privacy breach (i.e. law enforcement, insurers, regulatory bodies, other affected parties and the BC OIPC).

Step 4: Preventing Future Breaches

Once the risks associated with the breach have been mitigated, the Guidance Document recommends that organizations investigate the cause of the breach and determine what is needed to prevent a similar incident from occurring again. In this regard, the BC OIPC recommends that organizations review and update current policies and continue to do so regularly.

Key Takeaway

British Columbia currently stands on its own as the only Canadian jurisdiction that does not have statutory breach reporting or notification requirements. Yet, the BC OIPC's recommendations in the Guidance Document acknowledge that notification to individuals can be a useful tool to mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed, and that notification to the BC OIPC may be appropriate in certain circumstances.

Given the significant business implications for organizations following a privacy breach, it is important to engage external counsel early in the process to obtain advice on applicable legal and regulatory requirements arising from a breach and to manage associated legal risks.

by Mitch Koczerginski, Yue Fei, and Lily Le (Articling Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.