Office of the Information and Privacy Commissioner of Alberta

Practice Note

OIPC Process for Determining Whether to Require Notification

This practice note is for private sector organizations under the *Personal Information Protection Act*.

Section 37.1 of the *Personal Information Protection Act* (PIPA) provides authority for the Commissioner to require an organization to notify individuals of a loss or unauthorized access or disclosure of personal information as follows:

> **Power to require notification**
>
> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure
>
> (a) in a form and manner prescribed by the regulations, and
> (b) within a time period determined by the Commissioner.

Section 37.1(3) of PIPA requires the Commissioner **to establish an expedited process for determining whether to require an organization to notify individuals** in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate. This document sets out that process.

Reporting a Breach to the Commissioner

An organization must notify the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information, where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the incident (section 34.1).

A report to the Commissioner must include the information prescribed by section 19 of the *Personal Information Protection Act Regulation* (PIPA Regulation; PIPA, section 34.1).

It is an offence to fail to provide notice to the Commissioner under section 34.1 (PIPA, section 59(1)(e.1)).

A report to the Commissioner must be made **in writing**, and must be submitted **without unreasonable delay** using one of the following methods. Please complete the Privacy Breach Report Form and follow the instructions to submit it.

OIPC Process

Upon receiving a report from an organization, the OIPC will open a report file, and assign a tracking number. A letter will be sent to the organization's contact acknowledging receipt of the report.

The OIPC will review the organization's report to ensure it includes all of the information required by section 19 of the PIPA Regulation:

- If the report is not complete, the OIPC will contact the organization and request that the organization submit a complete report.
- Upon being contacted by the OIPC, the organization must submit a complete report without unreasonable delay.

Once a completed report has been received, OIPC staff will forward the report file to the Commissioner.

The Commissioner will review the organization's report and the report file, and decide whether to require the organization to notify individuals to whom there is a **real risk of significant harm**.

If the Commissioner decides that the organization must notify affected individuals, the Commissioner may require that:

- The organization notify the individual(s) of the incident in a form and manner prescribed by the PIPA Regulation (PIPA, section 37.1(1)(a))
- Individuals be notified within a time period determined by the Commissioner (section 37.1(1)(b))
- The organization satisfy any additional terms or conditions that the Commissioner considers appropriate (section 37.1(2))

The Commissioner may require the organization to provide additional information in order to make a decision whether to require that the organization notify individuals (section 37.1(4)).

An organization is not restricted from notifying individuals on its own initiative (section 37.1(7)). However, in the event an organization has notified individuals on its own initiative before reporting an incident to the Commissioner, the Commissioner may, upon reviewing the organization's notice and finding it deficient, require the organization to notify individuals in the form and manner prescribed by the PIPA Regulation (if this has not been done) or to satisfy additional terms and conditions as determined by the Commissioner.

Note: Organizations should consider the requirements in section 19.1(1) of the PIPA Regulation when they are notifying individuals on their own accord of a breach. Where the Commissioner requires notification, if the notification given by the organization on its own does not meet the requirements of section 19.1(1) of the PIPA Regulation, the Commissioner may require (and has required) an organization to notify individuals again. There is also the possibility that the Commissioner may require an organization to provide additional notification other than that provided in section 19.1(1) in accordance with the authority in section 37.1(2).

Direct vs. Indirect Notification

Where the Commissioner requires an organization to notify an individual(s), the notification to the individual(s) must be given directly unless the Commissioner determines that direct notification would be unreasonable in the circumstances (PIPA Regulation, section 19.1).

If an organization believes that direct notification to individuals is likely to be unreasonable, the organization should give **reasons for this at the time the organization submits its Privacy Breach Report Form to the Commissioner**; doing so will help to expedite the decision-making process.

Commissioner's Decision

The Commissioner's written decision to require an organization to notify individuals will be issued to the organization within a reasonable time of the OIPC having received the organization's report of a breach that includes, at a minimum, the information required by section 19.1 of the PIPA Regulation.

Publishing Decisions

Pursuant to section 38(6) of PIPA, the Commissioner "may publish any finding or decision in a complete or an abridged form."

Where the Commissioner requires that an organization notify individuals to whom there is a real risk of significant harm, the Commissioner's decision will be published at www.oipc.ab.ca.

In the event the Commissioner decides that notification of individuals is not required an abridged version of the Commissioner's decision may be published.

Complaint Received

If the Commissioner receives a complaint from a person with respect to an incident that has already been reported to the Commissioner under section 34.1, the Commissioner will advise the person that the incident was reported, and that the Commissioner will make a decision as to whether the organization is required to notify individuals to whom there is a real risk of significant harm. The Commissioner may also initiate a separate investigation as a result of having received the complaint.

Other Resources

Additional resources are on the "How to Report Privacy Breach" webpage available at www.oipc.ab.ca.

For general information about responding to a privacy breach, please contact the OIPC by telephone at (780) 422-6860 or toll free at 1-888-878-4044. Information provided does not constitute legal advice, is not binding on the Commissioner, and does not mean an organization or custodian has fulfilled its legal obligation to report a privacy breach to the Commissioner.