Office of the Information and Privacy Commissioner of Alberta

OIPC PIPA Privacy Breach Process

Commissioner's Power to Require Notification

Under section 37.1, of the *Personal Information Protection Act* (PIPA) the Information and Privacy Commissioner (Commissioner) may require an organization to notify individuals to whom there is a real risk of significant harm as a result of the loss of or unauthorized access to or disclosure ("privacy breach") of the individuals' personal information. Section 37.1 states in part:

> 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.

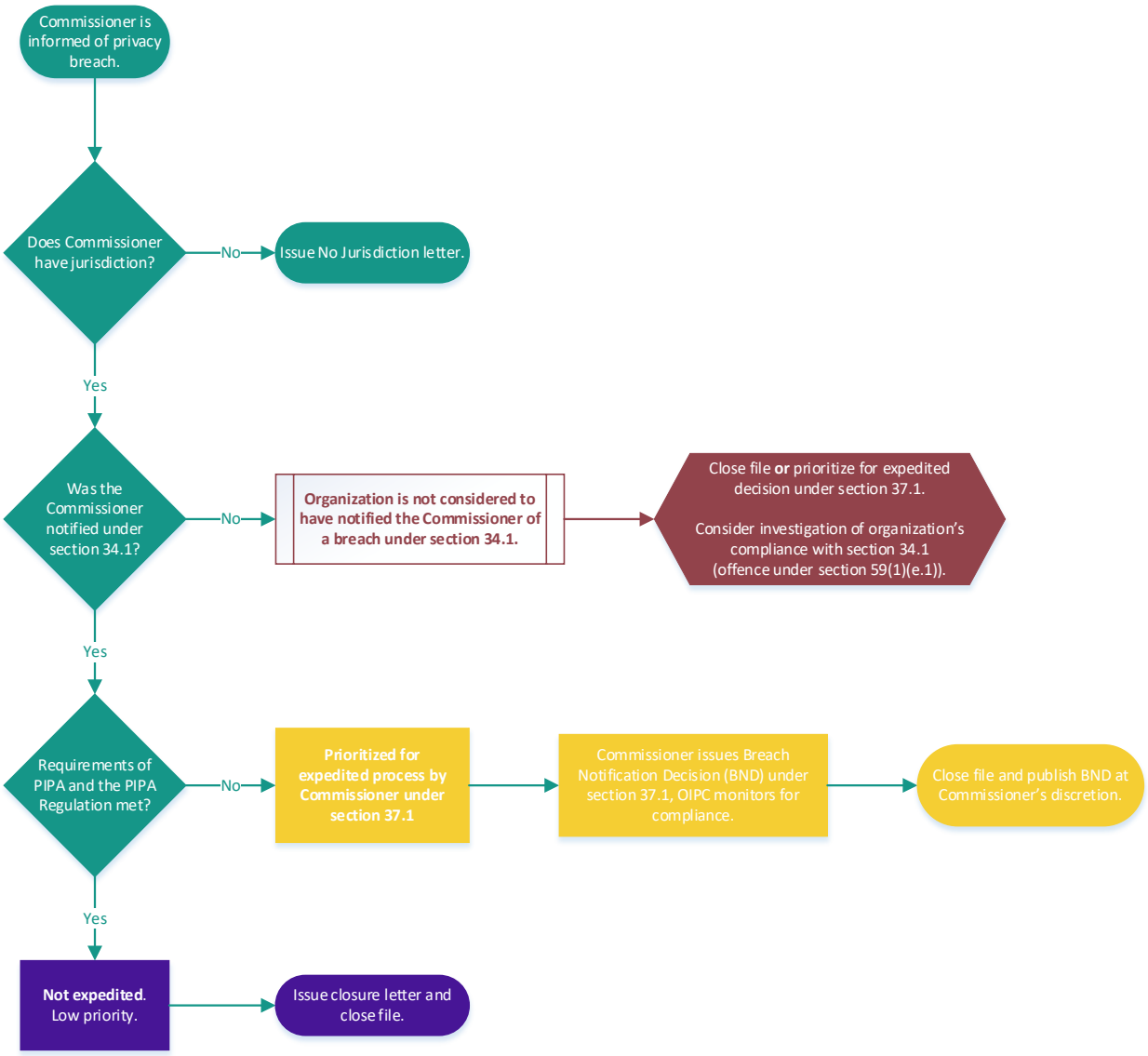
Section 37.1(3) of PIPA requires the Commissioner **to establish an expedited process for determining whether to require an organization to notify individuals** in the circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is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

In circumstances where an organization has **not notified affected individuals** and / or the Commissioner requires additional information about a privacy breach in order to decide whether to require the organization to notify affected individuals or establish additional terms or conditions (section 37.1(2)), the Commissioner may choose to exercise powers under section 37.1(4) to obtain that information.

This document describes the Commissioner's expedited process established under section 37.1(3).

Process for Determining Whether to Require an Organization to Notify Individuals

Simplified Overview of the Process



Detailed Description of the Process

Notifying the Commissioner

Organizations must, without unreasonable delay, notify the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of personal information under its control, where a reasonable person would consider that **there exists a real risk of significant harm** (RROSH) to an individual as a result of the loss or unauthorized access or disclosure (section 34.1).

Notice of a breach to the Commissioner under section 34.1(1) must be in **writing**, and must include the information prescribed by section 19 of the *Personal Information Protection Act Regulation* (the *PIPA Regulation*).

Triage and Case Prioritization

Upon receiving information about a breach from an organization, the OIPC opens a case file with a unique file number for reference purposes. The case file is triaged to determine whether:

- the Commissioner has jurisdiction,
- the organization is providing notice to the Commissioner under section 34.1 of PIPA,
- notice to the Commissioner meets the requirements of section 19 of the *PIPA Regulation*, and
- the organization notified individuals in accordance with section 19.1(1) of the *PIPA Regulation*.

The Office of the Information and Privacy Commissioner (OIPC) has developed the **PIPA Privacy Breach Notification Form** to assist organizations with notifying the Commissioner of a privacy breach.

The OIPC recommends that organizations use this form when notifying the Commissioner as it prompts the organization to notify the Commissioner in accordance with the requirements of section 19 of the *PIPA Regulation*.

Certain case files will be prioritized for a decision by the Commissioner. For example, cases where individuals have **not** been given notice in accordance with section 19.1(1) of the *PIPA Regulation* will be assigned a higher priority. For lower priority files, organizations may experience a delay prior to receiving requests for additional information under section 37.1(4), being required to notify or re-notify individuals, or to satisfy any terms or conditions under section 37.1(2).

Requests for Additional Information under 37.1(4)

The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization to notify individuals or satisfy terms and conditions (section 37.1(4)).

Where the Commissioner requires additional information, questions will be sent to the organization with a reasonable timeline to respond. Timelines are more urgent where individuals have not been notified and where the real risk of significant harm to an individual is obvious and immediate (37.1(3)). Pursuant to section 37.1(5)(a), It is critical that an organization respond without unreasonable delay to ensure the Commissioner has up to date information when issuing a decision.

The Commissioner may request additional information about an incident regardless of whether or not an organization has notified the Commissioner under section 34.1. Pursuant to section 37.1(5)(a), organizations must comply with a requirement to provide additional information under section 37.1(4).

Example Outcomes of the Process

Expedited, High Priority

Certain case files, typically involving an organization that has **not directly notified affected individuals** in accordance with the *PIPA Regulation*, will be prioritized for a Breach Notification Decision by the Commissioner. For example:

34.1 Notice – Individuals Not Notified

> An organization notifies the Commissioner under section 34.1 of an incident where a reasonable person would consider there exists a RROSH to individuals, but the Organization has **not** notified them.
>
> Organizations are not restricted from notifying individuals on their own initiative (section 37.1(7)), however, some organizations choose to wait for the Commissioner to issue a Breach Notification Decision under section 37.1(1) prior to directly notifying affected individuals in accordance with section 19.1 of the PIPA Regulation.

Non-34.1 Notice – Individuals Not Notified and RROSH to Individuals is Obvious and Immediate

> An organization provides information about a breach on an informal, voluntary, or courtesy basis to the Commissioner. However, the information describes an incident involving personal information collected in Alberta, where RROSH to an individual as a result of the loss of or unauthorized access to or disclosure of the personal information is obvious and immediate (section 37.1(3)), but the organization has not notified individuals.

34.1 Notice - Individuals Not Notified, Direct Notice Unreasonable

> In certain circumstances, direct notice to affected individuals may be unreasonable. Organizations may seek authorization from the Commissioner to notify individuals **indirectly** under section 19.1(2) of the *PIPA Regulation*.

34.1 Notice – Notice to Commissioner or Individuals does not meet Requirements of the PIPA Regulation

> An organization notifies the Commissioner under section 34.1 but does not provide enough detail; notice to the Commissioner does not meet one or more requirement of section 19 of the *PIPA Regulation*; or an organization's notice to affected individuals does not meet one or more requirement of section 19.1 of the *PIPA Regulation*.

In the above examples, the Commissioner may request additional information about the privacy breach which the Commissioner considers necessary to determine whether to require the organization to notify individuals under section 37.1(1), satisfy additional terms and conditions (section 37.1(2)), or determine if direct notification would be unreasonable in the circumstances (section 19.1(2) of the *PIPA Regulation*). Pursuant to section 37.1(5)(a), organizations must comply with a requirement to provide additional information under section 37.1(4).

Where the Commissioner requires an organization to notify affected individuals or satisfy additional terms and conditions, or authorize the indirect notification of individuals, the Commissioner may issue a written Breach Notification Decision under section 37.1(1).

Not Expedited, Low Priority

For lower priority files, organizations may experience a delay prior to receiving requests for additional information under section 37.1(4), being required to notify or re-notify individuals, or to satisfy any terms or conditions under section 37.1(2). Some examples include:

34.1 Notice: Individuals Notified, No Additional Information Required

> The organization notified the Commissioner of a privacy breach where a reasonable person would consider that there exists a real risk of significant harm to affected individuals under section 34.1 using the OIPC PIPA Privacy Breach Notification Form (Breach Form).
>
> The organization provided sufficient detail in its 34.1 notice to the Commissioner and notice to the Commissioner meets the requirements of section 19 of the *PIPA Regulation*.
>
> The organization notified affected individuals directly in accordance with section 19.1(1) of the *PIPA Regulation*.
>
> **The Commissioner may choose not to exercise powers under section 37.1. In that case, the OIPC will send a letter to the organization, acknowledging that the organization has directly notified individuals as required by section 19.1(1) of the *PIPA Regulation*.**

Non-34.1 Notice: Breach does not meet Real Risk of Significant Harm Threshold

> Notice provided to the Commissioner by an organization under section 34.1 describes a breach that the Commissioner would not consider to pose a real risk of significant harm to individuals.
>
> **The Commissioner may choose not to exercise powers under section 37.1. In that case, the OIPC will send a letter to the organization acknowledging the circumstances of the privacy breach, acknowledge whether the organization notified individuals, and indicate the Commissioner's view that the incident does not pose a real risk of significant harm to individuals.**

Other Outcomes

No Jurisdiction

In some circumstances, the Commissioner may not have jurisdiction to require notification under section 37.1. For example, certain privacy breaches involving non-profits, incidents that do not involve personal information collected in Alberta, or incidents involving organizations that are federal works, undertakings or businesses subject to the federal privacy legislation.

In this case, the OIPC may send a letter to the organization describing why the Commissioner does not have jurisdiction to require notification under section 37.1.

Informal, Voluntary, or Courtesy Letters from Organizations

Sometimes organizations will send to the Commissioner an informal or "courtesy" letter about a privacy breach, or inform the Commissioner about an incident where, in the organization's view, a reasonable person would not consider a real risk of significant harm to individuals exists.

If these informal letters do not contain the information required by section 19 of the *PIPA Regulation*, or if the organization does not indicate there exists real risk of significant harm, the organization is not considered to have notified the Commissioner under section 34.1.

When informing the Commissioner about a breach informally, whether in writing or verbally (such as by telephone or video conference), the organization is not considered to have notified the Commissioner under section 34.1.

In these cases, the Commissioner may require the organization to provide additional information about the privacy breach under section 37.1(4) to determine whether to require the organization to notify individuals or to establish additional terms and conditions. Pursuant to section 37.1(5)(a), organizations must comply with a requirement to provide additional information under section 37.1(4).

Alternatively, the OIPC may send a letter setting out the expectation that an organization notify the Commissioner under section 34.1 when the organization has determined a real risk of significant harm to individuals exists, triggering its duty to notify.

Information from Third Parties

Periodically, information about a breach is provided by third parties, such as affected individuals or news media, who are not authorized to report the breach on behalf of the organization having control of the affected personal information. These third party reports are also not considered to be notice to the Commissioner under section 34.1.

The Commissioner may contact the organization alleged to have experienced a breach, setting the expectation that the organization notify the Commissioner under section 34.1 when the organization has determined a real risk of significant harm exists, triggering its duty to notify.

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

The Commissioner may investigate whether an organization complied with its section 34.1 duty to notify the Commissioner of a privacy breach, as provided by section 36(1)(a) and section 36(2)(e.1).

Other Process Matters

Commissioner's Decision

The Commissioner's decision under section 37.1(1) is based on the information submitted by the Organization up to the date that the Commissioner makes a decision. The Organization is responsible for providing up to date information prior to a decision (section 37.1(5)).

Decisions are final and generally not subject to further comment or revision, based on the principle of *functus officio*. However, the Commissioner has said that the PIPA breach notification provisions contain an implied power to reconsider a decision. Therefore, an organization may make a formal written request to reconsider a decision. A request to reconsider a decision must address principles set out in *Chandler v. Alberta Association of Architects, [1989] 2 S.C.R. 848*.

Notifying Individuals Directly

An organization is not restricted from notifying individuals on its own initiative, pursuant to section 37.1(7) of PIPA. In the event that an organization has notified affected individuals of a privacy breach on its own initiative, where there exists a RROSH to the individuals, the Commissioner, upon considering the organization's notice, may require the organization to notify the affected individuals again in the form and manner prescribed by the *PIPA Regulation* or to satisfy additional terms and conditions (section 37.1(2)).

Note: Organizations should consider the requirements in section 19.1(1) of the *PIPA Regulation* when they are notifying affected individuals of a breach. Where the Commissioner requires notification, if the notification given by the organization 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 Commissioner's authority pursuant to section 37.1(2). See, for example, Breach Notification Decision P2023-ND-015,

Notifying Individuals Indirectly

Where the Commissioner requires an organization to notify an individual, notification must be given **directly** to the individual (*PIPA Regulation*, section 19.1(1)(a)). Pursuant to section 19.1(2), notification to an affected individual may be given **indirectly** if the Commissioner determines that direct notification would be unreasonable in the circumstances.

If an organization believes direct notification to individuals is unreasonable in the circumstances, the organization should give reasons why direct notification is unreasonable at the time it notifies the Commissioner. See, for example, Breach Notification Decisions P2021-ND-284, P2020-ND-172, and P2019-ND-127.

Complaints and Investigations

If the Commissioner receives a complaint from a person with respect to an incident about which the Commissioner has already been notified, the Commissioner may inform the person that the Commissioner was notified.

The Commissioner may initiate an investigation as a result of having received a complaint (section 36(2)), or on her own motion to ensure compliance with any provision of PIPA (section 36(1)(a)), including whether an organization complied with its duty to notify the Commissioner under section 34.1 (section 36(2)(e.1)).

Publishing under PIPA

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 decides to publish any report, finding, decision or summary, it will be published on the OIPC webpage.

Reports, findings, decisions, summaries or results of matters may be published for numerous reasons, such as to promote transparency, accountability and credibility of the OIPC; to educate the public; to promote the public interest; to establish precedent; and to meet the statutory requirement that the Commissioner, as an officer of the Legislature, report annually to the Speaker of the Legislative Assembly about the work of the OIPC under PIPA and other matters relating to the protection of personal information that the Commissioner considers appropriate.

General Publication of Section 37.1 Breach Notification Decisions

Mandatory breach notification under PIPA came into force on May 1, 2010. Since coming into force, the Commissioner's practice was to publish all section 37.1 Breach Notification Decisions (BNDs) in which an organization was required to notify individuals for whom there is a real risk of significant harm. Publishing BNDs enabled the creation of a body of knowledge, covering diverse scenarios across over 1,450 privacy breaches, which serves to educate Albertans and provide organizations with a resource for assessing real risk of significant harm as a result of a privacy breach.

As of the implementation of this updated process, the general publication of BNDs will cease until further notice. However, the Commissioner may decide to issue a BND under section 37.1(1). If so, the Commissioner may publish that BND in a complete or abridged form. The Organization affected by the BND will generally be informed prior to publication.

The Commissioner may publish abridged summaries of privacy breaches and statistical information about privacy breaches to inform Albertans of novel incidents and trends.

Other Resources

Additional resources are on the How to Notify the Commissioner of a Privacy Breach page on the OIPC website.

For general information about responding to a privacy breach, please contact the OIPC by telephone at (780) 422-6860, toll free at 1-888-878-4044, or by email at breachnotice@oipc.ab.ca. Contacting the OIPC does not mean that an organization has fulfilled its legal obligation to notify the Commissioner about a privacy breach. Notification to the Commissioner about a privacy breach must meet the requirements of section 19 of the PIPA Regulation. Information provided by the OIPC does not constitute legal advice and is not binding on the Commissioner.