Fact sheet: Privacy Incident Notifications

The *Protection of Privacy Act* (POPA) has requirements for notification in response to privacy incidents where there is a real risk of significant harm. This fact sheet provides guidance on how to determine if an incident meets the threshold for "real risk of significant harm," and the requirements for notices themselves.

Protection of Personal Information

POPA requires that the head of a public body protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction (section 10(1)).

Privacy Incidents

Should there be a loss, unauthorized access, or unauthorized disclosure where there is a real risk of significant harm as a result of a privacy incident as per section 10(2), the public body must give notice to the individual, Alberta's Information and Privacy Commissioner (the Commissioner), and the Minister responsible for this Act (the Minister of Technology and Innovation).

Section 10(2) states:

(2) If an incident occurs involving the loss of, unauthorized access to or unauthorized disclosure of personal information in the custody or under the control of a public body where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss, unauthorized access or unauthorized disclosure, the public body must give notice, without unreasonable delay, of the incident to the following:

(a) the individual to whom there exists a real risk of significant harm;

(b) the Commissioner;

(c) the Minister.

This requirement also applies to those incidents involving data derived from personal information that meet the threshold of a "real risk of significant harm" as described in section 10(2).

For the public body, taking appropriate steps to contain the incident and completing notification in a timely manner minimizes the harm that an incident may cause. Doing so also enables impacted individual(s) to take steps to further protect themselves and reduces the chance their information is misused.

Determining Real Risk of Significant Harm

The Protection of Privacy (Ministerial) Regulation defines "real risk of significant harm" (RROSH) by separately addressing "real risk of significant harm" overall, and "significant harm."

Section 4(1) of the regulation identifies factors constituting a "real risk of significant harm." Section 4(2) identifies various potential impacts considered to have a significant level of harm to an individual. Combined, these factors are intended to assist the public body in assessing the level of potential harm associated with the incident, and the likelihood or probability that this risk exists and may occur.

Of particular note, the level of sensitivity associated with the personal information involved in the incident, and any mitigating factors taken to reduce or mitigate the risk of harm must be considered. If any other relevant factors exist not included in the regulation, they should also be considered during the public body's assessment.

If, based on this assessment, it is determined that the incident meets the threshold for RROSH, the public body is required to complete notification. However, even if an incident does not meet the threshold for RROSH, public bodies may still choose to notify the impacted individual as a best practice measure, promoting transparency and accountability.

If you have questions on whether there exists RROSH, you may wish to contact the Office of the Information and Privacy Commissioner to discuss your specific incident.

Notification

As per section 10(3), any notice given under section 10(2) must comply with the prescribed requirements set out in the regulation. Notification must be completed without unreasonable delay.

The Protection of Privacy (Ministerial) Regulation outlines the notification requirements for the individual (section 4(3)), the Commissioner (section 4(4)), and the Minister (section 4(5)). These requirements vary for each recipient, tailored to their specific needs. For instance, the information to impacted individuals and

the Commissioner should be more detailed than notifications to the Minister.

When the regulation requires a “description” or “general description” of certain information in a notice (e.g., sections 4(3)(b)(v), 4(4)(b)(viii), 4(5)(b)(ii), etc.), public bodies must not include any actual personal information. For example, if an incident involved an individual’s date of birth, the description should only state, “date of birth,” not the specific date.

Furthermore, notices to the Commissioner and the Minister must not include any personal information about the impacted individual. For the Commissioner, this also applies to the copy of the notice provided to impacted individuals (section 4(4)(b)(xii)).

Manner of Notification

Public bodies must give written notice through one of the authorized methods listed in section 53 of POPA. These include, but are not limited to, sending directly to the recipient by prepaid mail to their last known address, or by electronic form other than fax, such as email, if that person’s contact information for that electronic form is publicly available or has been provided to the public body by that person.

Notice to the Commissioner

Please refer to the Office of the Information and Privacy Commissioner of Alberta’s website for more information on how to submit a notice to the Commissioner.

Notice to the Minister

Please refer to Report a Privacy Incident for more information on how to submit a notice to the Minister.

Data Derived from Personal Information

POPA also requires the head of a public body to also protect data derived from personal information from those same risks, i.e., unauthorized access, collection, use, disclosure or destruction (section 20).

Data derived from personal information is still recorded information about an identifiable individual, and therefore meets the definition of “personal information”. Public bodies are therefore required to provide notice under section 10(2) when an incident involves data derived from personal information and meets the threshold for a “real risk of significant harm.”

According to section 1(e), data derived from personal information refers to data created by data matching, that identifies any individual whose personal information was used in the data matching. Data matching, as defined in section 1(f), involves linking personal information between two or more databases or other electronic sources.

Based on these definitions, data derived from personal information ultimately consists of personal information about an identifiable individual as defined under section 1(q). Consequently, the loss of, or unauthorized access to or disclosure of such data may also result in significant harm to individuals. This type of incident therefore falls within the scope of a privacy incident as outlined in section 10(2).

For more information, refer to the Fact Sheet: Data Matching and Data Derived from Personal Information.

Privacy Management Programs

As part of their privacy management programs (PMPs), section 6(1)(b)(i)(B) of the regulation requires public bodies to establish internal policies and procedures for handling incidents as described in 10(2).

It is the responsibility of each public body to ensure that all employees — including contractors — are informed of, and understand, these policies and procedures, as well as their specific responsibilities related to privacy incident management and notification.

For contractors in particular, public bodies should incorporate privacy protection clauses in the contracts or agreements. These clauses must clearly define the service provider’s obligations in the event of a privacy incident.

Additionally, when public bodies participate in common or integrated programs or services, or engage in data matching initiatives, they must ensure that roles, responsibilities, and accountability for privacy incidents are clearly defined in the governance structure of the Privacy Impact Assessment, as required under section 7(2)(g).

Please refer to your internal policies and procedures for more information on how your public body handles these incidents and notification.