NATIONAL PRIVACY COMMISSION

The NPC is an attached agency of the Department of Information and Communications Technology

Personal Data Breach Management

A **personal data breach** is a breach of security resulting to accidental or unlawful destruction, loss, or alteration of personal data, including its unauthorized disclosure.

A **security incident** is an event or situation that affects or will likely affect data protection or compromise the availability, integrity, and confidentiality of personal data.

All personal data breaches are essentially security incidents.

A security incident will result in a personal data breach if there are no existing safeguards to remedy the situation.

There are three types of personal data breach.

Availability Breach — loss, accidental or unlawful destruction of personal data.

Integrity Breach — alteration of or unauthorized changes to personal data.

Confidentiality Breach — unauthorized disclosure of or access to personal data.

What to do in the event of a personal data breach

Initial Assessment of the Breach

- Identify the officer to lead the investigation
- Identify and take immediate action to stop the source of breach
- Determine the nature, extent, scope, and circumstances surrounding the breach
- Determine the possible personal data involved
- Ascertain the data subjects affected
- Document all initial information gathered for further investigation

Mitigation of the Impact of the Breach

- Restore the integrity of the system
- Change the encryption keys and passwords
- Isolate and preserve compromised data
- Attempt to retrieve lost or compromised data
- Prepare back-up mechanism
- Implement an inquiry and assistance hotline for data subjects
- Secure all evidence and reports
- Coordinate and cooperate witih law enforcement agencies

Notification regarding the Breach

- Notify the National Privacy Commission and the affected data subjects
- The obligation to notify lies with the Personal Information Controller even when the processing is outsourced

Notification to the Commission

... must be sent within 72 hours upon knowledge of or the reasonable belief that a personal data breach has occurred. The Commission must be notified based on available information even if the full extent of the breach is not yet known if the personal data breach involves at least 100 data subjects or the disclosure of sensitive personal information will harm data subjects. In other cases, notification may be delayed if the scope of the breach cannot be determined within the 72-hr period, or if it is necessary to prevent further disclosure or to restore system integrity.

.... must contain (1) Nature, extent and impact of the breach; (2) Personal data possibly involved; (3) Measures taken to address the breach; (4) Details of the Data Protection Officer or contact person designated by the Personal Information Controller to provide additional information; and (5) Any assistance to be provided the data subject.

Full report to the Commission

... must be submitted within 5 days upon knowledge or occurrence of the breach, unless granted additional time by the Commission.

Notification to Data Subjects

... must be sent individually, by written or electronic means.

.... must include (a) instructions on how data subjects will get further information; and (b) recommendations on how to minimize risks resulting from breach. The Commission, upon request, may allow exemption or postponement of notification of data subjects if the notification would not be in the public interest or the interest of data subjects.

The National Privacy Commission and, as a general rule, affected data subjects must only be notified in the event of a personal data breach. Security incidents will only be included in an annual report to be submitted to the Commission by personal information controllers. Notification shall be mandatory when the following are present:

It involves sensitive personal information or that may be used for identity fraud.

Information may have been acquired by an unauthorized person or group of people.

It is likely to give rise to a real risk of serious harm to the affected data subjects.

When there is doubt as to the need to notify, consider if it
— would likely affect national security, public safety, public order, or public health
— involves at least 100 individuals
— are required by laws or rules to be confidential
— pertain to vulnerable groups

What must be done after the occurrence of a personal data breach?

- Produce a comprehensive report of the breach.
- Assess the adequacy of the actions and decision of the data breach response team.
- Determine the gaps and evaluate effectiveness of policies and procedures.
- Conduct trainings and workshops for personnel involved in processing.
- Update technology and systems for efficiency.
- Evaluate incident mitigation mechanism.
- Provide assistance to data subjects affected by breaches.
- Solicit feedback from data subjects on how to improve the breach response procedure.
- Adjust the organizational, physical and technical security measures.
- Continue to monitor risk communications and discovery and reporting methods.