PERSONAL DATA PROTECTION COMMISSION SINGAPORE

AN INTRODUCTION TO MANAGING DATA BREACHES 2.0

A data breach refers to an incident exposing personal data in an organisation's possession or under its control to unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Having a data breach management plan in place enables organisations to respond swiftly in managing any data breaches in a systematic manner.

The plan should include the following sets of activities:

C ontaining the Breach

A ssessing Risks and Impact

R eporting the Incident

E valuating the Response and Take Actions to Prevent Future Breaches

The complete Guide to Managing Data Breaches 2.0 can be downloaded at www.pdpc.gov.sg/og

STEP 1

Contain

Staff should **report** all suspected/confirmed data breaches immediately to the data breach management team that has expertise in handling personal data and data breaches.

Data Intermediaries should report data breaches to the main organisation without undue delay (**no later than 24 hours**) from the time it first becomes aware of the breach.

The team should conduct an **initial assessment** to determine the severity of data breach:

- Cause of the data breach and whether the breach still ongoing
- Number of individuals affected
- Types of personal data disclosed
- Systems and/or services affected
- Whether help is required to contain the breach

Act swiftly to **contain** the breach (i.e. taking **immediate** steps to limit any further access to or disclosure of the personal data).

Record the data breach and the organisation's response(s) in an Incident Record Log.

STEP 2

Assess

An **in-depth** assessment of the extent and likely impact of the data breach can help an organisation identify and take the appropriate steps to limit the impact of the breach. Organisations should then be able to conclude whether the data breach is **unlikely or likely** to result in causing significant harm to the affected individuals, and take steps to reduce any potential harm to the affected individuals if necessary.

When **assessing the breach**, consider the following:

- Circumstances of the data breach, including its cause and extent
- Types of personal data involved
- Number and groups of affected individuals
- Risks involved
- Whether external help is required
- Remedial actions which can be taken if deemed necessary

When **evaluating risks** posed by the data breach, consider the following:

- Sensitivity of the data involved
- Presence of mitigating factors (e.g. encryption)
- What happened to the data
- Nature of harm to the affected individuals (if any)

STEP 3

Report

NOTIFY PDPC when

Significant harm or impact is likely
or
500 or more individuals affected

Organisations should notify **PDPC as soon as practicable, no later than 72 hours** from the time the organisation has made its assessment.

Organisations may send an **email*** to notify the PDPC of the data breach.

NOTIFY AFFECTED INDIVIDUALS when

Significant harm or impact is likely

Organisations should **also notify affected individuals as soon as practicable**. Notifications should include (but not be limited to) the following*:

- Specific facts on the data breach
- Actions individuals can take
- Organisation's contact details

* Refer to complete Guide to Managing Data Breaches 2.0 for more details

STEP 4

Evaluate

Review and take action to prevent future breaches. This may include the following:

- Implementation/continuing efforts of the remediation actions
- Identification of areas of weakness and taking action to strengthen them
- Effectiveness of the organisation's data breach response(s)
- Corrective actions to be taken

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CSA SINGAPORE

In support of: SG:D EMPOWERING POSSIBILITIES

10 Pasir Panjang Road #03-01 Mapletree Business City, Singapore 117438
Main Line: +65 6377 3131 • Fax: +65 6577 3888 • www.pdpc.gov.sg