pdpc

PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

GUIDE TO MANAGING DATA BREACHES

8 MAY 2015

CONTENT

PURPOSE OF THIS GUIDE

This Guide aims to help organisations manage personal data breaches effectively.

NOTICE

While the examples in this guide touch on various aspects of the Protection Obligation in the Personal Data Protection Act ("PDPA"), they do not address every obligation in the PDPA that would apply in each example.

Organisations should consider their own circumstances and requirements as well as other PDPA obligations, when managing data breaches.

INTRODUCTION

What is a data breach? A data breach generally refers to the unauthorised access and retrieval of information that may include corporate and personal data.

Why it is important to prevent and manage data breaches

Data breaches are generally recognised as one of the more **costly** security failures of organisations. They could lead to financial losses, and cause consumers to lose trust in an organisation.

The Personal Data Protection Act 2012 ("PDPA") requires organisations to make **reasonable security arrangements** to protect the personal data that they possess or control, to prevent unauthorised access, collection, use, disclosure or similar risks.

Organisations may be **subject to other** sector-specific rules under laws that require them to complement or further protect personal data.

Some organisations may also have **common law duties** that require them to keep certain information confidential. This information may include personal data.

HOW DATA BREACHES COULD OCCUR

Data breaches can occur for different reasons. They may be caused by employees, parties external to the organisation or computer system errors. Possible ways in which a data breach may occur are:

Malicious Activities

- Hacking incidents / Illegal access to databases containing personal data
- Theft of computer notebooks, data storage devices or paper records containing personal data
- Scams that trick organisations into releasing personal data of individuals

Human Error

- Loss of computer notebooks, data storage devices or paper records containing personal data
- Sending personal data to a wrong e-mail or physical address, or disclosing data to a wrong recipient
- Unauthorised access or disclosure of personal data by employees
- Improper disposal of personal data (e.g. hard disk, storage media or paper documents containing personal data sold or discarded before data is properly deleted)

Computer System Error

- Errors or bugs in the programming code of websites, databases and other software which may be exploited to gain access to personal data stored on computer systems

RESPONDING TO A DATA BREACH

i. Data Breach Management Plan

Organisations should develop and implement a data breach management and response plan to manage data breaches. The plan may include the following sets of activities:

C ontaining the Breach

A ssessing Risks and Impact

R eporting the Incident

E valuating the Response & Recovery to Prevent Future Breaches

An organisation's data breach management and response plan may also include:

- **Details of the data breach management team**, with a clear command and reporting structure of key employees who would take charge and make time-critical decisions on steps to be taken to contain the breach and manage the incident.

- **Circumstances under which the data breach management team would be alerted of any data breach**. Information should also include the contact details of the management team and when the team would be activated to manage a data breach situation.

- **Possible data breach scenarios and how to respond to them.**

ii. Containing the Breach

An organisation should act as soon as it is aware of a data breach. It should consider the following measures, where applicable:

Shut down the compromised system that led to the data breach.

Establish whether steps can be taken to recover lost data and limit any damage caused by the breach.
(e.g. remotely disabling a lost notebook containing personal data of individuals.)

Prevent further unauthorised access to the system. Reset passwords if accounts and passwords have been compromised.

Put a stop to practices that led to the data breach.
(e.g. shredding paper documents containing personal data instead of throwing into the garbage bin.)

Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system and remove external connections to the system.

Address lapses in processes that led to the data breach.

Notify the police if criminal activity is suspected and preserve evidence for investigation.
(e.g. hacking, theft or unauthorised system access by an employee.)

iii. Assessing Risks and Impact

Knowing the risks and impact of data breaches will help organisations determine whether there could be serious consequences to affected individuals, as well as the steps necessary to notify the individuals affected. Here are some considerations:

Risk and Impact on Individuals

- **How many people were affected?**
    - A higher number may not mean a higher risk, but assessing this helps overall risk assessment.
- **Whose personal data had been breached?**
    - Does the personal data belong to employees, customers or minors? Different people will face varying levels of risk as a result of a loss of personal data.
- **What types of personal data were involved?**
    - This will help to ascertain if there are risk to reputation, identity theft, safety and/or financial loss of affected individuals.
- **Any additional measures in place to minimise the impact of a data breach?**
    - E.g. a lost device protected by a strong password or encryption could reduce the impact of a data breach.

Risk and Impact on Organisations

- **What caused the data breach?**
    - Determining how the breach occurred (through theft, accident, unauthorised access, etc.) will help organisations identify immediate steps to take to contain the breach and restore public confidence in a product or service.
- **When and how often did the breach occur?**
    - Examining this will help organisations better understand the nature of the breach (e.g. malicious or accidental).
- **Who might gain access to the compromised personal data?**
    - This will ascertain how the compromised data could be used. In particular notification to affected individuals would be required if personal data is acquired by an unauthorised person.
- **Will compromised data affect transactions with any other third parties?**
    - Determining this will help identify if other organisations need to be notified.

iv. Reporting the Incident

In general, it is a good practice to notify individuals affected by a data breach. Not only will this encourage individuals to take preventive measures to reduce the impact of the data breach, it will also help an organisation rebuild consumer trust. Organisation could also be bound by legal or contractual obligations to notify affected individuals.

Who to Notify?

- Notify individuals whose personal data have been compromised. This includes guardians or parents of young children whose personal data have been compromised.
- Notify other third parties such as banks, credit card companies or the police, where relevant.
- Notify PDPC especially if a data breach involves sensitive personal data.

When to Notify?

- Notify affected individuals immediately if a data breach involves sensitive personal data. This allows them to take necessary actions early to avoid potential abuse of the compromised data.
- Notify affected individuals when the data breach is resolved.

How to Notify?

- Adopt the most effective ways to reach out to affected individuals, taking into consideration the urgency of the situation and number of individuals affected (e.g. media releases, social media, e-mails, telephone calls, faxes and letters).
- Notifications should be simple to understand, specific and provide clear instructions on what individuals can do to protect themselves.

What to Notify?

- How and when the data breach occurred, types of personal data involved in the data breach.
- What the organisation has done or will be doing in response to the risks brought about by the data breach.
- Specific facts on the data breach where applicable, and actions individuals can take to prevent that data from being misused or abused.
- Contact details and how affected individuals can reach the organisation for further information or assistance (e.g. helpline numbers, e-mail addresses or websites).

Reporting the Incident to the Personal Data Protection Commission

- Organisations are advised to notify PDPC as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals.

- Details of data breaches can be sent to the PDPC at info@pdpc.gov.sg with the e-mail subject "[Data Breach Notification]". For urgent notification of major cases, organisations may also contact the Commission at +65 6377 3131.

- The notification should include the following information, where available:
  - Extent of the data breach
  - Type and volume of personal data involved
  - Cause or suspected cause of the breach
  - Whether the breach has been rectified
  - Measures and processes that the organisation had put in place at the time of the breach
  - Information on whether affected individuals of the data breach were notified and if not, when the organisation intends to do so
  - Contact details of persons whom the PDPC could liaise with for further information or clarification

- Where specific information of the data breach is not yet available, organisations should send an interim notification comprising a brief description of the incident.

- Notifications made by organisations or the lack of notification, as well as whether organisations have adequate recovery procedures in place, will affect PDPC's decision on whether an organisation has reasonably protected the personal data under its control or possession.

v. Evaluating the Response and Recovery to Prevent Future Breaches

After steps have been taken to resolve the data breach, organisations should review the cause of the breach and evaluate if existing protection and prevention measures are sufficient to prevent similar breaches from occurring. Organisations may wish to consider the following areas:

Operational and Policy Related Issues	• Were **audits regularly conducted** on both physical and IT-related security measures? • Are there **processes that can be streamlined or introduced** to limit the damage if future breaches happen or to prevent a relapse? • Were there **weaknesses in existing security measures** such as the use of outdated software and protection measures, or weaknesses in the use of portable storage devices or connectivity to the Internet? • Were the methods for accessing and transmitting **personal data sufficiently secure, e.g., access limited** to authorised personnel only? • Should **support services from external parties be enhanced**, such as vendors and partners, to better protect personal data? • Were the **responsibilities of vendors and partners clearly defined** in relation to the handling of personal data? • Is there a need to **develop new data-breach scenarios**?
Resource Related Issues	• Were there **enough resources** to manage the data breach? Should external resources be engaged to better manage such incidents? • Were **key personnel given sufficient resources** to manage the incident?
Employee Related Issues	• Were **employees aware** of security related issues? • Was **training provided** on personal data protection matters and incident management skills? • Were **employees informed of the data breach** and the learning points from the incident?
Management Related Issues	• How **was management involved** in the management of the data breach? • Was there a **clear line of responsibility and communication** during the management of the data breach?

CONCLUSION

Managing data breaches is important to protect the personal data of individuals when a data breach occurs. The Commission encourages organisations to pro-actively prepare and implement a good data breach management and response plan. Organisations should continuously review the plan to ensure it remains effective and relevant as business operations evolve.

For more information on the PDPA, or to view our other guides and advisory guidelines, please visit www.pdpc.gov.sg.

BROUGHT TO YOU BY

pdpc
PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

IN PARTNERSHIP WITH

CSA
SINGAPORE

This publication gives a general introduction to managing data breaches. The contents herein are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. The Personal Data Protection Commission (PDPC), the Info-communications Development Authority of Singapore (IDA) and their respective members, officers and employees shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.