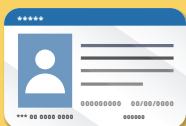


# Guidance on Data Breach Handling and Data Breach Notifications



PCPD



H K

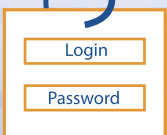
PCPD.org.hk

香港個人資料私隱專員公署  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong



## WHAT IS A DATA BREACH?

A data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user, which exposes the personal data of data subject(s) to the risk of unauthorised or accidental access, processing, erasure, loss or use. It may amount to a contravention of Data Protection Principle 4 – security of personal data of the Personal Data (Privacy) Ordinance.



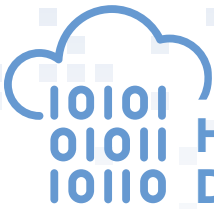


# DATA BREACH RESPONSE PLAN

A data breach response plan sets out how an organisation will respond in the event of a data breach. A comprehensive data breach response plan ensures a quick response to and effective management of a data breach, which may substantially minimise and contain the impact of the breach.

## Essential elements of a Data Breach Response Plan

- **Description of what constitutes a data breach**
- **Internal incident notification procedure** to alert senior management, the data protection officer and/or the data breach response team
- **Designation of the roles and responsibilities** of the data breach response team members
- **Contact details** of data breach response team members
- **Risk assessment workflow** to assess harm to affected data subjects
- **Containment strategy** for containing and remedying the breach
- **Communication plan** to determine whether and how data subjects, regulatory authorities and/or other relevant parties should be notified
- **Investigation procedure** for investigating the breach and reporting to senior management
- **Record-keeping policy** to properly document the incident
- **Post-incident review mechanism** to identify improvement to prevent recurrence
- **Training or drill plan** to ensure all relevant staff can follow the procedures properly when dealing with a data breach



# HANDLING DATA BREACHES

## STEP 1

### Immediate gathering of essential information

Gather all relevant information of the data breach to assess the impact on data subjects and to identify appropriate mitigation measures.

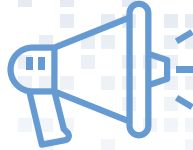
- When and where did the breach occur?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind of personal data was involved?
- How many data subjects might be affected? What harm may have been caused to them?

## STEP 2

### Containing the data breach

Depending on the severity of the breach and the personal data involved, this may include:

- Conducting a thorough search for the lost items containing personal data
- Changing users' passwords and system configurations to block any (further) unauthorised access
- Fixing any bugs that may have caused the breach
- Alerting banks etc to reduce the risk of financial losses for affected data subjects
- Notifying law enforcement agencies if identity thefts or other criminal activities are likely
- Shutting down or isolating compromised systems and checking whether other interconnected systems are affected
- Removing access rights of users suspected to have contributed to the breach

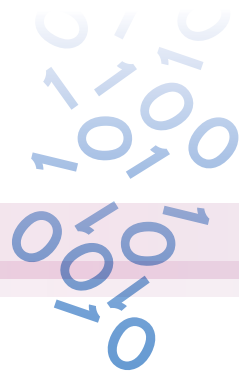


### STEP 3

## Assessing the risk of harm

Assess the possible harm that may be caused to individuals, such as:

- Threats to personal safety
- Identity theft
- Financial loss, or loss of business or employment opportunities
- Humiliation, loss of dignity, damage to reputations



### STEP 4

## Considering giving data breach notifications

As soon as practicable after becoming aware of the data breach, particularly when there is a real risk of harm to the affected data subjects, should:

- Notify the PCPD
- Notify affected data subjects and relevant parties

### STEP 5

## Documenting the breach

A comprehensive record of the incident would facilitate post-breach reviews and improve personal data handling practices.

# WHAT IS A DATA BREACH NOTIFICATION?

A data breach notification is a formal notification given by the data user to the relevant parties including the affected data subjects and regulators such as the PCPD. A notification should generally be given as soon as practicable after becoming aware of the incident, regardless of the progress of any internal investigation. Data users are advised to use the PCPD's Data Breach Notification Form when reporting a data breach to the PCPD. The Form may be submitted online, by fax, in person or by post.



Unit 1303, 13/F., Dah Sing Financial Centre,  
248 Queen's Road East, Wanchai, Hong Kong

Tel: 2827 2827  
Fax: 2877 7026  
E-mail: [communications@pcpd.org.hk](mailto:communications@pcpd.org.hk)  
Website: [www.pcpd.org.hk](http://www.pcpd.org.hk)



Download this  
Publication



Download the  
Guidance Note




e-Data Breach  
Notification Form



This publication is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this publication, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit [creativecommons.org/licenses/by/4.0](http://creativecommons.org/licenses/by/4.0).

First published in August 2023

 Printed on recycled paper