# Data Breach Notification Form

A data breach is generally taken to be a breach of the security of the personal data held by a data user, which results in exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use. Depending on the circumstances of the case, the breach in question may amount to a contravention of Data Protection Principle 4 of the Personal Data (Privacy) Ordinance (the Ordinance).

Although it is not mandatory under the Ordinance for data users to give data breach notifications, data users are encouraged to give such notifications timely to the Office of the Privacy Commissioner for Personal Data (PCPD), the affected data subjects and other relevant parties when a data breach has occurred.

This notification form is for a data user to report a data breach to the PCPD and it may take about 10-15 minutes to complete. You may refer to our "Practical Tips for Handling Data Breach Incident" at Annex for more information.

## Personal Information Collection Statement

Please be advised that it is voluntary for you to supply to the PCPD your personal data. All personal data submitted will only be used for purposes which are directly related to this data breach notification and the exercise of the regulatory powers and functions of the Privacy Commissioner for Personal Data.

You have the right to request access to and correction of your personal data held by the PCPD. Request for access or correction of personal data should be made in writing to the Data Protection Officer at the address: 12/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong.

The personal data submitted may be transferred to parties who may be contacted by the PCPD during the handling of this case including agencies who are authorised to receive information relating to law enforcement or prosecution.

❑ **I understand the above and I would like to submit a data breach notification on behalf of a data user.***

* Mandatory # Please circle as appropriate

## BASIC INFORMATION OF THE DATA USER

**User Sector :** ❑ Private Sector ❑ Public Sector

**Company/organisation name*:** _____

**Hong Kong office's correspondence address :** _____

_____

## INFORMATION OF THE CONTACT PERSON

**Name of person making this notification*:** Mr / Ms / Miss # _____

**Job Title :** _____ **Email address* :** _____

**Country code (for non-Hong Kong phone number) :** _____

**Contact phone number* :** _____

**Are you the Data Protection Officer for your company/organisation?** # Yes / No

## PARTICULARS OF THE DATA BREACH INCIDENT

**This is a new notification / an update of a previous notification.*#**

**Date of the data breach :** _____ (dd/mm/yyyy)

**When did your company/organisation become aware of the data breach?***
_____ (dd/mm/yyyy)

**Number of individuals affected*:** Please specify : _____

**Are there any Hong Kong residents affected?*#** Yes / No / To be confirmed

**Number of Hong Kong residents affected*:** Please specify : _____

**Types of personal data involved* :**

| | | |
|---|---|---|
| ❑ Name | ❑ Hong Kong identity card number | ❑ Passport number |
| ❑ Photograph | ❑ Date of birth | ❑ Address |
| ❑ Email Address | ❑ Telephone number | ❑ Health information |
| ❑ Financial information | ❑ Employment information | ❑ Social media account information |
| ❑ Academic information | ❑ Others, please specify : _____ | |

**Did you engage a service provider / contractor to handle the above personal data?** # Yes / No

**Details of the data breach*:**
(Summary of the cause/suspected cause of incident and how your organisation first became aware of the breach)

## ASSESSMENT OF THE INCIDENT AND REMEDIAL ACTIONS TAKEN

**Cause/Suspected Cause of incident* :**

❑ Accidental Disposal ❑ Cyberattack (e.g. hacking) ❑ Email Leakage

❑ Postal Leakage ❑ Loss of Physical Documents ❑ Loss of Electronic Devices

❑ Employee Misconduct ❑ Program Bug ❑ Server Misconfiguration

❑ Burglary ❑ Others, please specify : _____

**Real Risks to Data Subject(s)* :**

❑ Threat to personal safety ❑ Identity theft ❑ Financial loss

❑ Damage to reputation ❑ Loss of business opportunities ❑ Loss of employment opportunities

❑ No real risk of harm to data subject(s) ❑ Others, please specify : _____

**Summary of the remedial actions taken*:**

_____

_____

_____

_____

_____

**Were the affected individuals notified? *#** Yes / No / No, will do so within (____) days

**Has your company/organisation issued or does your company/organisation intend to issue a media statement? *#** Issued / Intend to issue / No

**Have any other authorities been notified of the data breach? (e.g. Hong Kong Police Force) *#** Yes / No

**Summary of the notification made to other authorities (if applicable)* :**

_____

_____

_____

_____

Please submit the completed form and other relevant documents concerning the data breach (if any) by the following channels:

- **By Post / In Person**
  Address: Room 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong
- **By Fax**
  Fax number: 2877 7026
- **By Email**
  Email address: dbn@pcpd.org.hk

Signature : _____

Name : _____

Job Title : _____

Date : _____

# Practical Tips for Handling Data Breach Incident

Annex

| **Data Breach Incident** | Accidental Disposal / Loss of Physical Document or Electronic Storage Device |
|---|---|
| **Immediate Remedial Measures** | • Try to locate the lost document / portable storage device as soon as possible<br>• If recovering the lost document / portable storage device is unsuccessful, contact the data subjects immediately |
| **Measures for Preventing Future Recurrence** | • Use designated bags with secured zip / lock to transit document with personal data<br>• Store document / device in a locked cabinet / drawer<br>• Maintain a record keeping track of document movement<br>• Use less printout and adopt digitalisation of document as far as practicable<br>• Arrange centralised destruction exercise regularly<br>• Seek management's approval before the use of portable storage device<br>• Install Mobile Device Management software which can wipe the data from the portable storage device remotely if it is lost<br>• Purge the personal data upon fulfilment of the original collection purpose |
| **Data Breach Incident** | Cyberattack (e.g. Hacking / Brute Force Attack / Ransomware Attack etc.) |
| **Immediate Remedial Measures** | • Disconnect the compromised device from the Internet and any network to which it is linked<br>• Perform an offline complete scan of the computer network using anti-virus software. Ignore any pop-ups telling you to connect to the Internet. If any malware is found, follow the software's instructions on how to quarantine or remove the malicious files<br>• Change login details for the compromised device / software / database / system<br>• Notify the relevant law enforcement agencies if identity theft or other criminal activities are or suspected to be committed |
| **Measures for Preventing Future Recurrence** | • Install a two tier firewall and enable end-point protection<br>• Use most updated version of operating systems and anti-virus programs<br>• Apply the latest security patches and virus signatures for all devices, including offline virtual machines<br>• Set a limit on the number of requests in a minute to a user login page from a single IP address<br>• Set up CAPTCHA[1] on the login page to guard against brute force attacks<br>• Do back up on a regular basis<br>• Carry out network segmentation by dividing the corporate network into subnets and dedicating each subnet to specific needs and functions. Only those with "a need-to-know" can access specified domains |

1. A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. For example, humans can read distorted text but computer programs cannot.

| **Data Breach Incident** | Email or Postal Leakage |
|---|---|
| **Immediate Remedial Measures** | • Try to recall the email / retrieve the letter if possible<br>• If recalling / retrieving is unsuccessful, contact and request the unintended recipients to delete the email / destroy the letter immediately |
| **Measures for Preventing Future Recurrence** | • Adopt four-eyes principle (i.e. counter-check the document by different staff) to ensure that all recipients' names, contact information, content and / or attachments are correct<br>• Use open-window envelope for posting if possible<br>• Minimise the kinds of personal data contained in an email<br>• Disable autocomplete function of the email system to prevent sending email to a similar but incorrect email address<br>• Name files properly in the first place such that the file name can truly reflect the content with an aim to minimising the chance of attaching wrong document in an email<br>• Use shared drive for internal transfer of files containing personal data<br>• Use strong password to protect email attachments containing personal data. Provide the recipient with the password of the attachment by another means |
| **Data Breach Incident** | Staff Misconduct |
| **Immediate Remedial Measures** | • Disable the account / access right of the staff concerned<br>• Notify the relevant law enforcement agencies if criminal activities are or likely to be committed |
| **Measures for Preventing Future Recurrence** | • Install Data Loss Prevention system / tool to scan external outgoing emails and quarantine those with sensitive information, such as HKID number and credit card details. Management's approval is required before the release of the quarantined email<br>• Allow authorised access to personal data only on a case-by-case basis, need-to-use basis or role-based approach<br>• Lock up restricted and confidential document at all time<br>• Review the system log records proactively to detect any irregularity at an early stage<br>• Perform full IT audit on departing staff upon their cessation of employment |

| **Data Breach Incident** | Phishing |
|---|---|
| **Immediate Remedial Measures** | • Disconnect the compromised device from the Internet and any network to which it is linked<br>• Perform an offline complete scan of the computer network using anti-virus software. Ignore any pop-ups telling you to connect to the Internet. If any malware is found, follow the software's instructions on how to quarantine or remove the malicious files<br>• Change login details for the compromised device / software / database / system |
| **Measures for Preventing Future Recurrence** | • Do not respond to any email that request you to provide login details or sensitive information (e.g. bank account details)<br>• Avoid opening any suspicious email attachment<br>• Carefully check the email address domain name for suspicious email<br>• Hover over a URL in an email to see the true destination before clicking to ensure legitimacy<br>• Install anti-phishing and anti-spam software<br>• Arrange personal data security awareness training to staff |
| **Data Breach Incident** | Program Bug or System Misconfiguration |
| **Immediate Remedial Measures** | • Disable the access to the concerned program / system / platform<br>• Contact the responsible vendor immediately if the concerned program / system / platform is developed / maintained by a third party |
| **Measures for Preventing Future Recurrence** | • Perform tests (including integrated tests, user acceptance test) to verify the program / system before moving it to the production environment<br>• Carry out vulnerability scanning and penetration testing to the system regularly and after any significant changes<br>• Check proper permissions have been set for files and folders on a regular basis<br>• Enter contract / agreement with a vendor with good reputation and track record in the industry. The contract / agreement must incorporate robust privacy protection requirements |