



Data Breach Notification Form

Notice

Notification of a data breach to the Privacy Commissioner for Personal Data, Hong Kong (the “**Commissioner**”) by the data user (*see Note 1*) is not a legal requirement. In deciding whether or not to give this notification to the Commissioner, you should consider the “Guidance on Data Breach Handling and the Giving of Breach Notifications” issued by the Commissioner. In most cases, it is advisable to give notifications to the data subject(s) (*see Note 2*) affected by the breach.

PARTICULARS OF THE PERSON GIVING THIS NOTIFICATION (i.e. the data user)

Name: _____

Address: _____

Telephone number: _____ Fax number: _____

Email address: _____

Where the person giving this notification is an organization, please provide the following information:

Contact person :

Name (*Mr./Ms./Miss): _____

Relationship with the Reporting Organization (e.g. job title): _____

Telephone number: _____ Fax number: _____

Email address: _____

(*Please delete as appropriate)

DETAILS ABOUT THE DATA BREACH (*see Note 3*):

ACTIONS TAKEN / WILL BE TAKEN TO CONTAIN THE BREACH (*see Note 4*)

Please set out details of any actions / measures taken or will be taken to mitigate and minimize the breach

RISK OF HARM (*see Note 5*)

Is there a real risk of harm to any individual? (Please tick one of the following boxes) Yes No

Please explain below why there is / there is no real risk of such harm

ASSISTANCE AND ADVICE OFFERED TO INDIVIDUALS

Describe (i) what has been done to inform the individual(s) affected by the breach; and (ii) if their safety, well-being or property is at risk as a result of the breach, what has been done or can be done to assist them in avoiding / mitigating that risk or its consequences

NOTIFICATION TO OTHER BODIES / REGULATORS / LAW ENFORCEMENT AGENCIES

Please provide details if such notification has been given

Signature: _____

Name: _____

Title: _____

Date: _____

Information Notes

- 1) Under section 2(1) of the Personal Data (Privacy) Ordinance (the “**Ordinance**”), “data user”, in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.
- 2) Under section 2(1) of the Ordinance, “data subject”, in relation to personal data, means the individual who is the subject of the data.
- 3) Please provide the following information as specific as possible:
 - ✓ What was the personal data concerned?
 - ✓ How many data subjects were/could be affected by the data breach?
 - ✓ What is the nature of the data breach (e.g. leakage, loss, unauthorized use, etc)?
 - ✓ When, where and how did the data breach take place?
 - ✓ What was the duration of the data breach?
 - ✓ When, where, how and by whom was the data breach discovered?
 - ✓ What was the cause of the data breach?
- 4) Containment measures may include:
 - ✓ Stopping the system if the data breach is caused by system failure
 - ✓ Changing the users’ passwords and system configurations to control access and use
 - ✓ Consider whether technical advice or assistance be immediately sought internally or from outside to remedy the system loopholes and/or stop the hacking
 - ✓ Ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach
 - ✓ Notifying the relevant law enforcement agencies if identity theft or other criminal activities were or likely to be committed
 - ✓ Keeping the evidence of the data breach which may be useful to facilitate investigation and the taking of corrective actions
 - ✓ In the event that the data breach was caused by the act or omission of the data processor, requiring the data processor to take immediate remedial measures and to notify the data user of the progress
- 5) The potential harm caused by the data breach may include:
 - ✓ Threat to personal safety
 - ✓ Identity theft
 - ✓ Financial loss
 - ✓ Humiliation or loss of dignity, damage to reputation or relationship
 - ✓ Loss of business and employment opportunities
- 6) Personal Information Collection Statement

Please be advised that it is voluntary for you to supply to the Office of the Privacy Commissioner for Personal Data, Hong Kong (the “**PCPD**”) your personal data. All personal data submitted will only be used for purposes which are directly related to this notification and the exercise of the regulatory powers and functions of the Commissioner. 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 shown in Note 7 below. 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 authorized to receive information relating to law enforcement or prosecution.

- 7) The address of the PCPD is at 12/F, Sunlight Tower, 248 Queen’s Road East, Wanchai, Hong Kong, and the office hours are: Monday - Friday 8:45 a.m. - 5:40 p.m., Saturday, Sunday and Public Holidays closed. (Enquiry hotline: 2827 2827, Fax: 2877 7026, Website: www.pcpd.org.hk)