PRIVACY AWARENESS WEEK 關注私隱運動

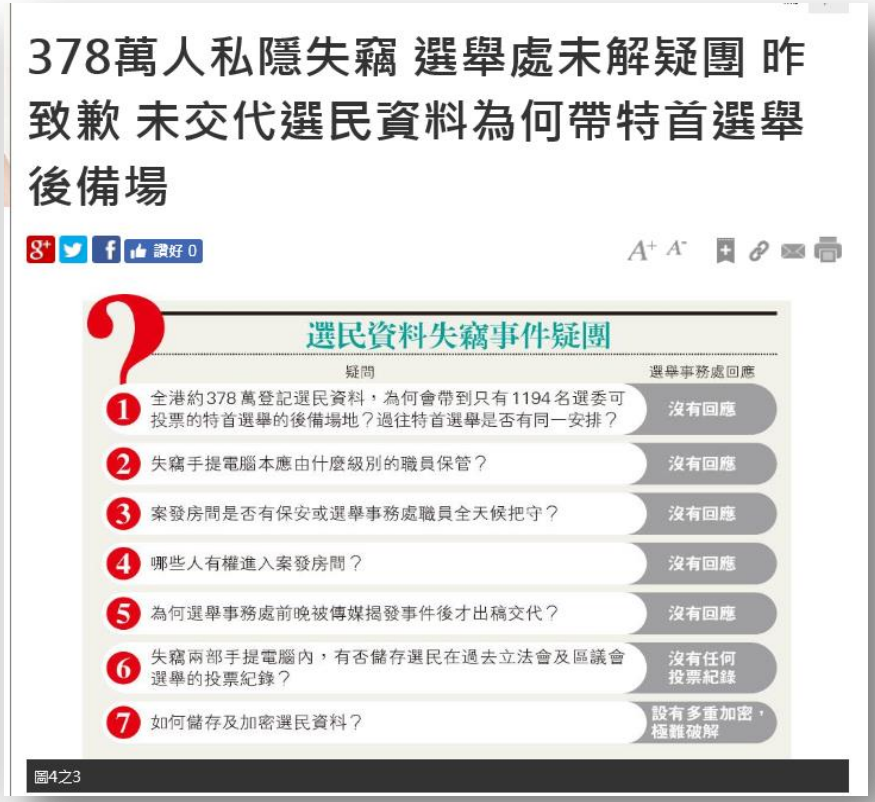
Privacy Awareness Week 2017
9 May 2017

Smart Use of Portable Storage Devices and Data Breach Handling

保障資料主任聯會 DATA PROTECTION OFFICERS' CLUB

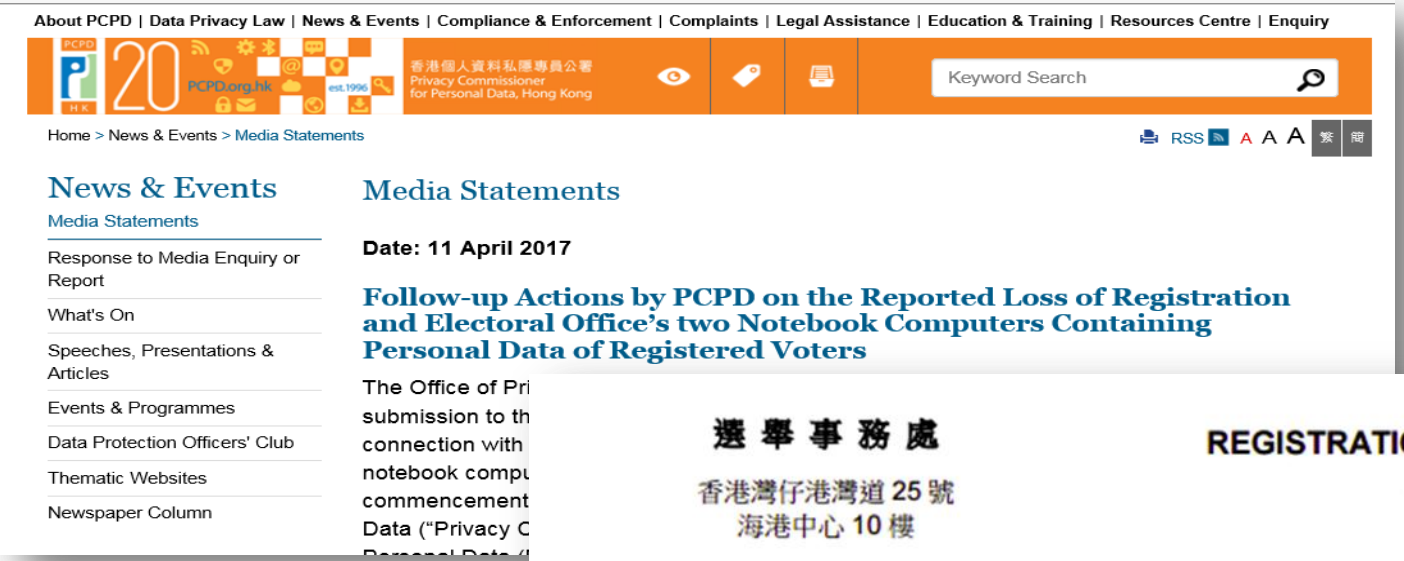
Recent Incidents

source: https://goo.gl/AyAAEk



source: https://goo.gl/IH0JFh

Recent Incidents



About PCPD | Data Privacy Law | News & Events | Compliance & Enforcement | Complaints | Legal Assistance | Education & Training | Resources Centre | Enquiry

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

Keyword Search

Home > News & Events > Media Statements

RSS A A A 繁 簡

News & Events

Media Statements

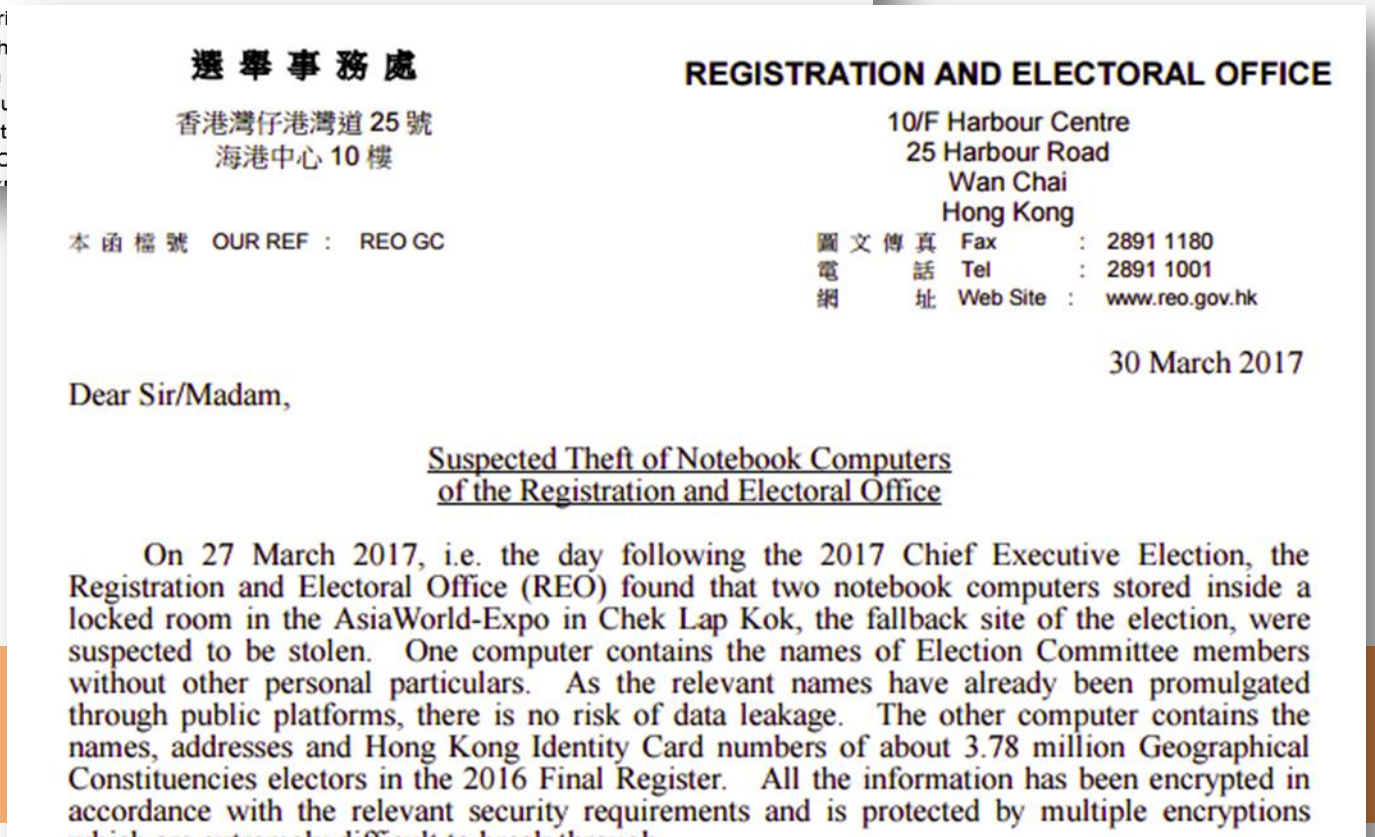
- Response to Media Enquiry or Report
- What's On
- Speeches, Presentations & Articles
- Events & Programmes
- Data Protection Officers' Club
- Thematic Websites
- Newspaper Column

Media Statements

Date: 11 April 2017

Follow-up Actions by PCPD on the Reported Loss of Registration and Electoral Office's two Notebook Computers Containing Personal Data of Registered Voters

The Office of Pri
submission to th
connection with
notebook compu
commencement
Data ("Privacy C



選舉事務處

香港灣仔港灣道 25 號
海港中心 10 樓

REGISTRATION AND ELECTORAL OFFICE

10/F Harbour Centre
25 Harbour Road
Wan Chai
Hong Kong

本函檔號 OUR REF : REO GC

圖文傳真 Fax : 2891 1180
電話 Tel : 2891 1001
網址 Web Site : www.reo.gov.hk

30 March 2017

Dear Sir/Madam,

Suspected Theft of Notebook Computers of the Registration and Electoral Office

On 27 March 2017, i.e. the day following the 2017 Chief Executive Election, the Registration and Electoral Office (REO) found that two notebook computers stored inside a locked room in the AsiaWorld-Expo in Chek Lap Kok, the fallback site of the election, were suspected to be stolen. One computer contains the names of Election Committee members without other personal particulars. As the relevant names have already been promulgated through public platforms, there is no risk of data leakage. The other computer contains the names, addresses and Hong Kong Identity Card numbers of about 3.78 million Geographical Constituencies electors in the 2016 Final Register. All the information has been encrypted in accordance with the relevant security requirements and is protected by multiple encryptions

PCPD HK PCPD.org.hk est.1996

Recent Incidents

source: https://goo.gl/CaZUXI

source: https://goo.gl/IHaFk5

Examples of Portable Storage Devices (PSDs)

The Six Data Protection Principles (DPPs)

6 保障資料原則 Data Protection Principles

PCPD.org.hk

1 收集目的及方式 Collection Purpose & Means

資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性儲存及保留 Accuracy & Retention

資料使用者須確保持有的個人資料準確無誤，資料的保留時間不應超過達致原來目的的實際所需。

Personal data is accurate and is not kept for a period longer than is necessary to fulfill the purpose for which it is used.

3 使用 Use

個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

Personal data is used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent is obtained from the data subject.

4 保安措施 Security

資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

A data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5 透明度 Openness

資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

A data user must make known to the public its personal data policies and practices, types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

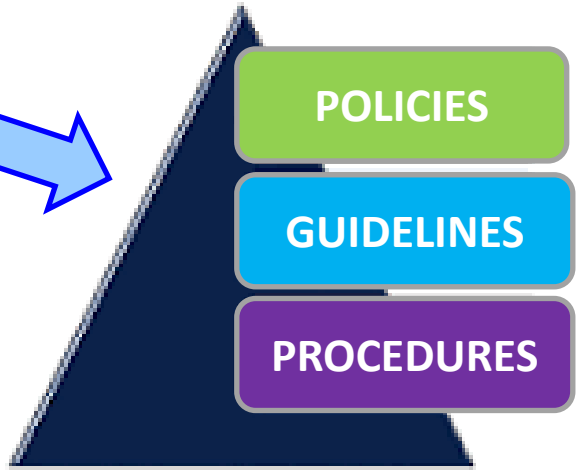
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

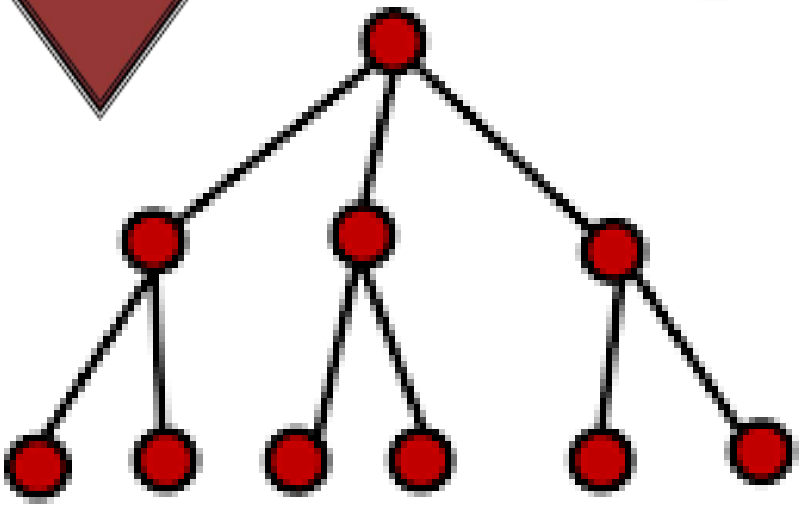
Data Protection Principle 4
Data Security Principle

- practicable steps to ensure no unauthorised or accidental access, processing, erasure, loss, use and transfer

- data users should take steps to manage the security risks associated with the use of PSDs

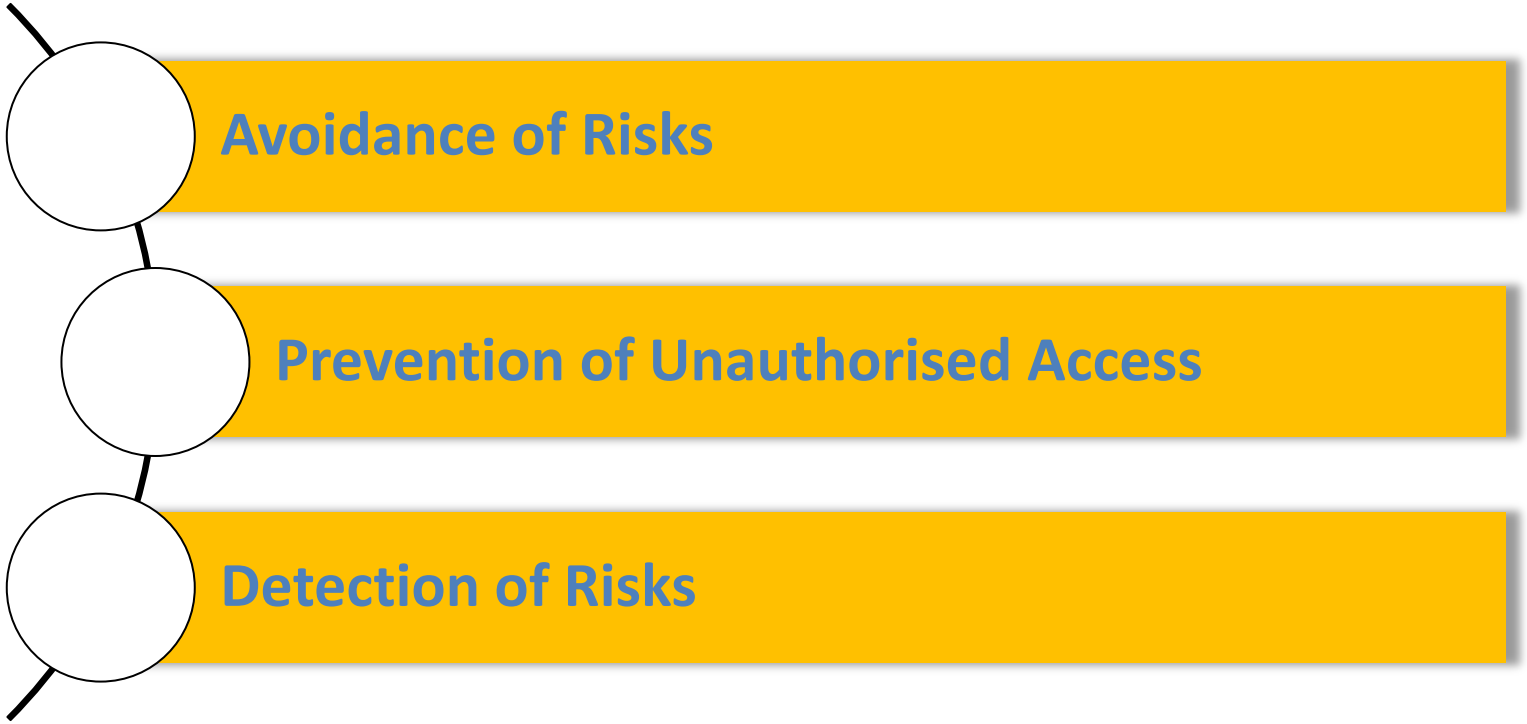
Smart Use of PSDs





Smart Use of PSDs

What should policy include?



Smart Use of PSDs

Avoidance of Risks

- ban the use of PSDs
- use internal identifies instead of HKID Card Number
- limit scope and detail of data
- devise policy
- erase data permanently before disposal

Smart Use of PSDs

Prevention of Unauthorised Access

encryption

password management

erase data securely

access control

Smart Use of PSDs

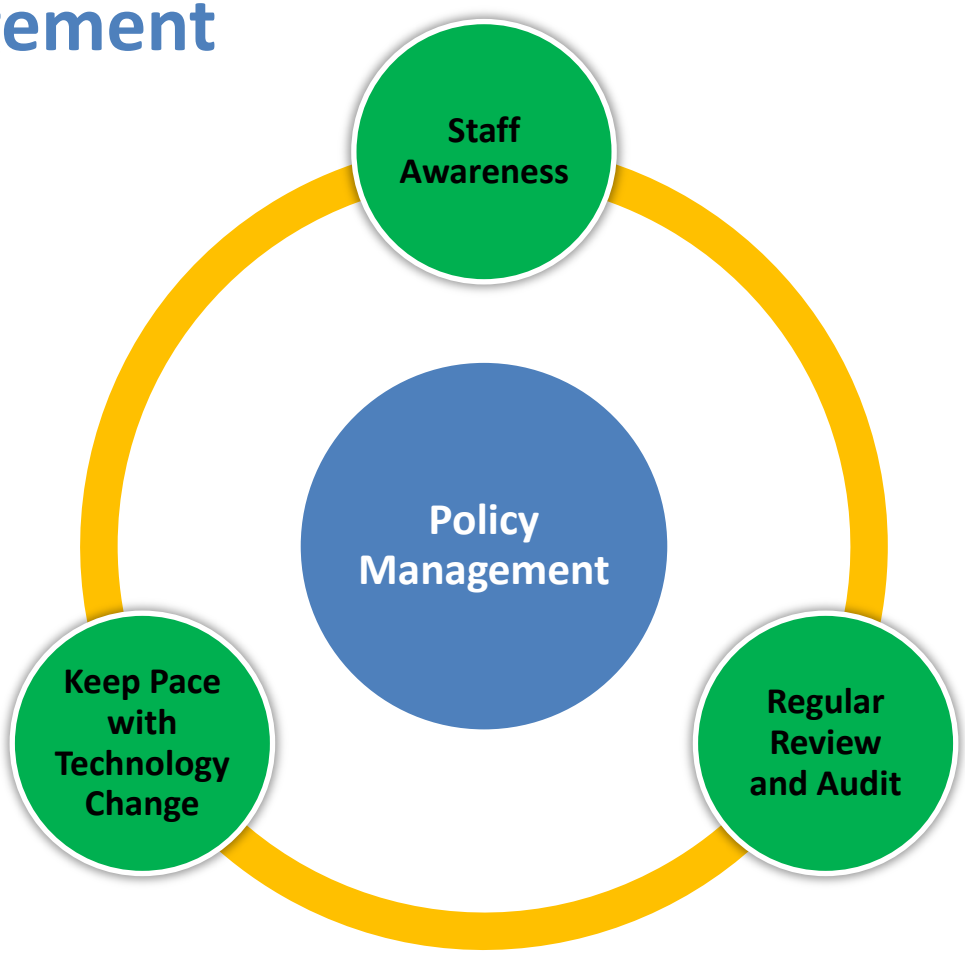
Detection of Risks

inventory checks/spot checks

loss reporting

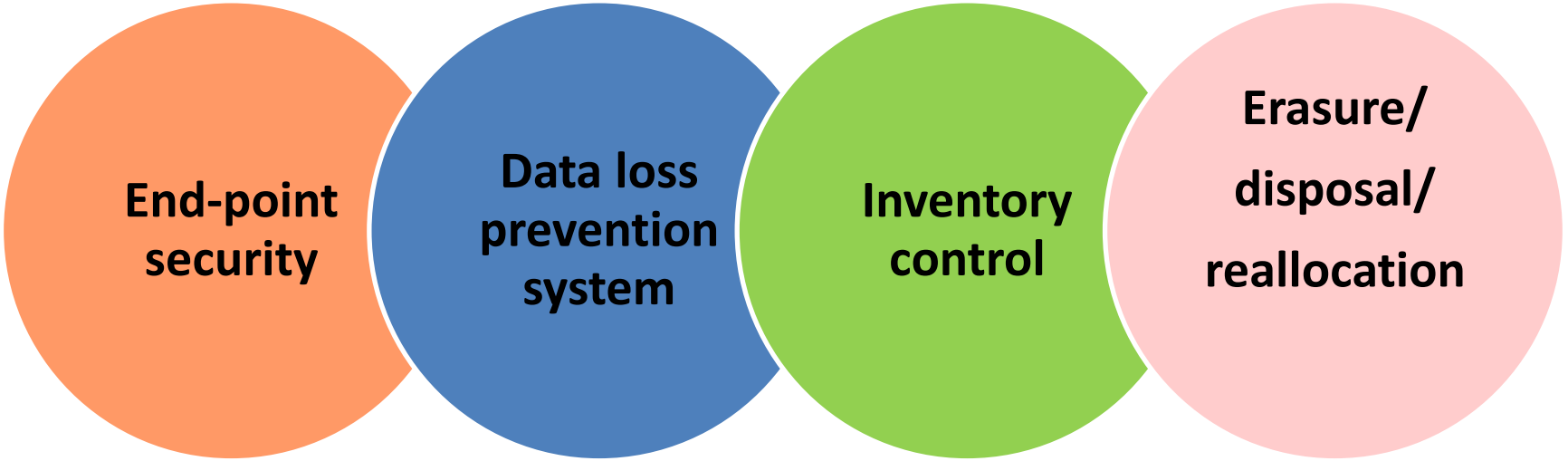
Smart Use of PSDs

Policy Management

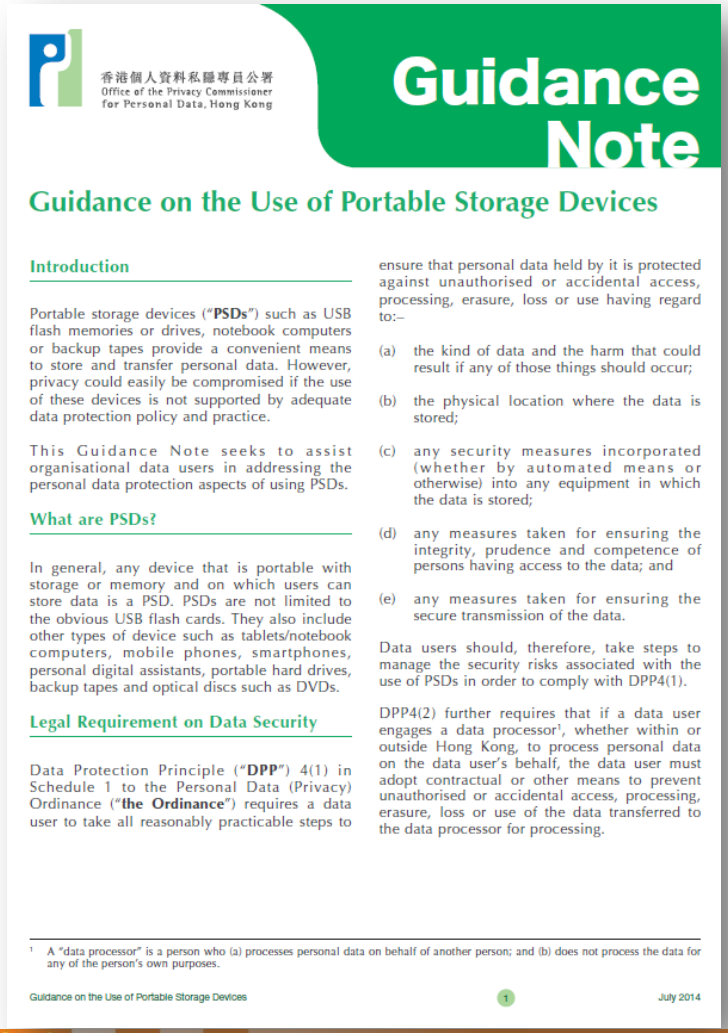


Smart Use of PSDs

Technical Control



Guidance on the Use of Portable Storage Devices



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

Guidance Note

Guidance on the Use of Portable Storage Devices

Introduction

Portable storage devices ("**PSDs**") such as USB flash memories or drives, notebook computers or backup tapes provide a convenient means to store and transfer personal data. However, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policy and practice.

This Guidance Note seeks to assist organisational data users in addressing the personal data protection aspects of using PSDs.

What are PSDs?

In general, any device that is portable with storage or memory and on which users can store data is a PSD. PSDs are not limited to the obvious USB flash cards. They also include other types of device such as tablets/notebook computers, mobile phones, smartphones, personal digital assistants, portable hard drives, backup tapes and optical discs such as DVDs.

Legal Requirement on Data Security

Data Protection Principle ("**DPP**") 4(1) in Schedule 1 to the Personal Data (Privacy) Ordinance ("**the Ordinance**") requires a data user to take all reasonably practicable steps to ensure that personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use having regard to:–

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data is stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and

(e) any measures taken for ensuring the secure transmission of the data.

Data users should, therefore, take steps to manage the security risks associated with the use of PSDs in order to comply with DPP4(1).

DPP4(2) further requires that if a data user engages a data processor[1], whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

[1] A "data processor" is a person who (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes.

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

指引資料

使用便攜式儲存裝置指引

導言

便攜式儲存裝置如USB記憶體、筆記型電腦或備份磁帶，為儲存及轉移個人資料提供了方便的途徑。不過，倘若沒有足夠的資料保障政策及措施規限此等裝置的使用，會增加私隱外洩的風險。

本指引旨在協助機構資料使用者在了解使用便攜式儲存裝置時，如何處理及保障個人資料。

甚麼是便攜式儲存裝置？

一般而言，任何可攜帶，並備有儲存或記憶功能的裝置，即屬便攜式儲存裝置。便攜式儲存裝置不限於USB記憶體，亦包括其他裝置類別，如平板／筆記型電腦、流動／智能電話、電子手帳、便攜式硬碟機，備份磁帶及光碟（例如DVD）。

資料保安的法律規定

《個人資料（私隱）條例》（下稱「**條例**」）附表1的保障資料第4(1)原則規定，資料使用者須採取所有合理地切實可行的步驟，以確保其持有的個人資料受保障而不受未獲准許或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮：

(a) 該資料的種類及如該等事情發生可造成的損害；

(b) 儲存該資料的地點；

(c) 儲存該資料的設備所包含（不論是藉自動化方法或其他方法）的保安措施；

(d) 為確保能查閱該資料的人的良好操守、審慎態度及辦事能力而採取的措施；及

(e) 為確保在保安良好的情況下傳送該資料而採取的措施。

因此，資料使用者應採取步驟，管理有關使用便攜式儲存裝置的保安風險，以遵從保障資料第4(1)原則的規定。

保障資料第4(2)原則進一步規定，如資料使用者聘用（不論是在香港或香港以外聘用）資料處理者[1]，以代行處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。

了解風險

容許使用便攜式儲存裝置，意味着大量的個人資料可以在不經意間快速及輕易地被複製到裝置內。若此等裝置遺失或盜竊，會產生資訊保安的風險，個人資料有可能會遭受未獲准許或意外的查閱或使用。在極端的例子中，即使便攜式儲存裝置已被重新格式化，過往被刪除或曾經儲存的個人資料亦可輕易地還原。

由上而下的策略

機構要管理有關使用便攜式儲存裝置的風險，應由上而下採取貫徹機構的政策。為方便制定政策，應首先進行風險評估。風險評估最少應涉及下述範疇：

(a) 儲存個人資料的便攜式儲存裝置是甚麼類型？

[1] 資料處理者指符合以下兩項說明的人－ (a) 代另一人處理個人資料；及(b) 並不為該人本身目的而處理該資料。

Data Breach

What is a data breach?

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, exposing the data 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.

source: https://goo.gl/EKtTxl

source: https://goo.gl/eGb6zn

source: https://goo.gl/di5uvn

Data Breach Handling

Collecting Information Immediately

Immediate gathering of essential information relating to the breach including:

- When and where did the breach take place?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind and extent of personal data was involved?
- How many data subjects were affected?

Data Breach Handling

Contacting the Interested Parties & Adopting Containment Measures

Interested parties may include:

- The law enforcement agencies
- The relevant regulators (e.g. Privacy Commissioner for Personal Data, Hong Kong (the "Commissioner"))
- The Internet companies
- IT experts

Containment measures may include:

- Stopping the system if the data breach is caused by a system failure
- Changing the users' passwords and system configurations to control access and use
- Considering whether technical assistance is needed 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 criminal activities are or likely to be committed
- Keeping the evidence of the data breach to facilitate investigation
- Directing the data processor to take immediate remedial measures and requesting it to notify the data user of the progress, if applicable

Data Breach Handling

Assessing the Harm

Assessing the potential harm caused by a data breach, for examples:

- Threat to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationship
- Loss of business and employment opportunities

Data Breach Handling

Considering the Giving of Notification

When real risk of harm is reasonably foreseeable in a data breach, the data user should consider:

- Notifying the affected data subjects and the relevant parties
- The consequences for failing to give notification

Data Breach Notification

What is a data breach notification?

A data breach notification is a formal notification given by the data user to the data subjects affected and the relevant parties and regulators in a data breach.

While it is not a statutory requirement on data users to inform the Office of the Privacy Commissioner for Personal Data, Hong Kong about a data breach incident concerning the personal data held by them, data users are nevertheless advised to do so as a recommended practice for proper handling of such incident.

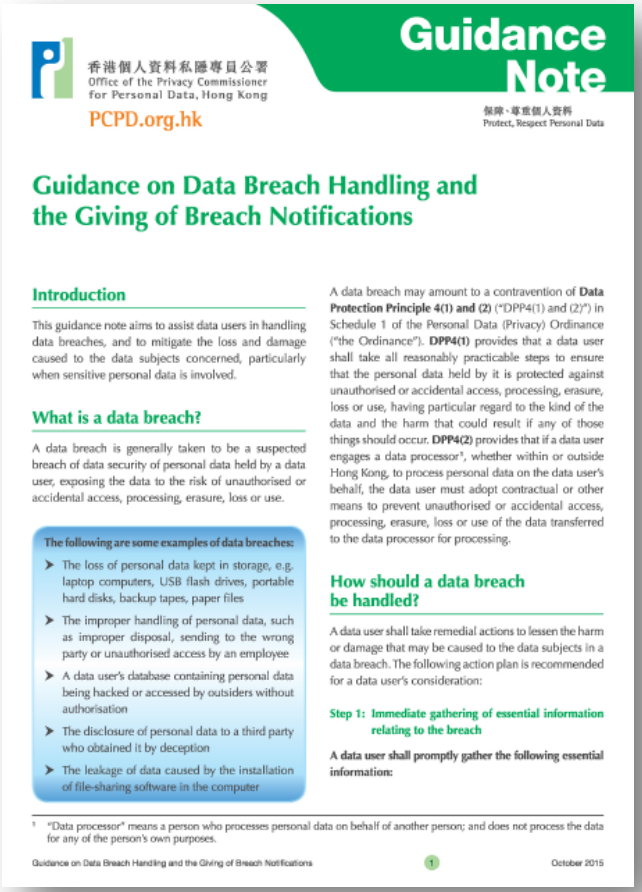
If a data user decides to report a data breach to the Commissioner, the data user may complete a Data Breach Notification Form and submit the completed form to us online, by fax, in person or by post.

Lesson Learnt to Prevent Recurrence

- improvement of security
- control of access rights
- revision or promulgation of privacy policy and practice
- effective detection of data breach
- Strengthening of monitoring and supervision
- Provision of on-the-job training

LESSON LEARNT

Guidance on Data Breach Handling and the Giving of Breach Notifications



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

Guidance Note

保障、尊重個人資料
Protect, Respect Personal Data

Guidance on Data Breach Handling and the Giving of Breach Notifications

Introduction

This guidance note aims to assist data users in handling data breaches, and to mitigate the loss and damage caused to the data subjects concerned, particularly when sensitive personal data is involved.

What is a data breach?

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

The following are some examples of data breaches:

- The loss of personal data kept in storage, e.g. laptop computers, USB flash drives, portable hard disks, backup tapes, paper files
- The improper handling of personal data, such as improper disposal, sending to the wrong party or unauthorised access by an employee
- A data user's database containing personal data being hacked or accessed by outsiders without authorisation
- The disclosure of personal data to a third party who obtained it by deception
- The leakage of data caused by the installation of file-sharing software in the computer

A data breach may amount to a contravention of **Data Protection Principle 4(1) and (2)** ("DPP4(1) and (2)") in Schedule 1 of the Personal Data (Privacy) Ordinance ("the Ordinance"). **DPP4(1)** provides that a data user shall take all reasonably practicable steps to ensure that the personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use, having particular regard to the kind of the data and the harm that could result if any of those things should occur. **DPP4(2)** provides that if a data user engages a data processor[1], whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

How should a data breach be handled?

A data user shall take remedial actions to lessen the harm or damage that may be caused to the data subjects in a data breach. The following action plan is recommended for a data user's consideration:

Step 1: Immediate gathering of essential information relating to the breach

A data user shall promptly gather the following essential information:

[1] "Data processor" means a person who processes personal data on behalf of another person; and does not process the data for any of the person's own purposes.

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

指引資料

保障、尊重個人資料
Protect, Respect Personal Data

資料外洩事故的處理及通報指引

導言

本指引旨在協助資料使用者處理資料外洩事故及減低對有關資料當事人所造成的損失及損害，尤其當事故涉及敏感個人資料。

甚麼是資料外洩事故？

資料外洩事故一般指資料使用者持有的個人資料懷疑外洩，令此資料有被未獲准許的或意外的查閱、處理、刪除、遺失或使用的風險。

下列是一些資料外洩事故的例子：

- 遺失儲存的個人資料，例如筆記電腦、USB記憶體、便攜式硬碟、備份磁帶、文件檔案
- 不當處理個人資料，例如不當地棄置、把資料錯誤地發給他人或僱員未獲准許而查閱資料
- 資料使用者載有個人資料的資料庫遭黑客入侵或遭外人未經授權查閱
- 第三者以欺騙手法從資料使用者取得個人資料
- 在電腦安裝檔案分享軟件而導致資料外洩

資料外洩事故可構成違反《個人資料（私隱）條例》（下稱「條例」）附表1的**保障資料第4(1)及(2)原則**，保障資料第4(1)原則規定資料使用者須採取所有切實可行的步驟，確保由資料使用者持有的個人資料受保障而不受未獲准許的或意外的查閱、處理、刪除、喪失或使用所影響，尤其須考慮該資料的種類及如該等事情發生可能造成的損害。保障資料第4(2)原則規定，如資料使用者聘用（不論是在香港或香港以外聘用）資料處理者[1]，以代該資料使用者處理個人資料，該資料使用者須採取合約規範方法或其他方法，以防止轉移予該資料處理者作處理的個人資料未獲准許或意外地被查閱、處理、刪除、喪失或使用。

如何處理資料外洩事故？

資料使用者應採取補救措施以減低資料外洩事故對資料當事人可能造成的傷害或損害。現建議下述行動計劃供資料使用者考慮：

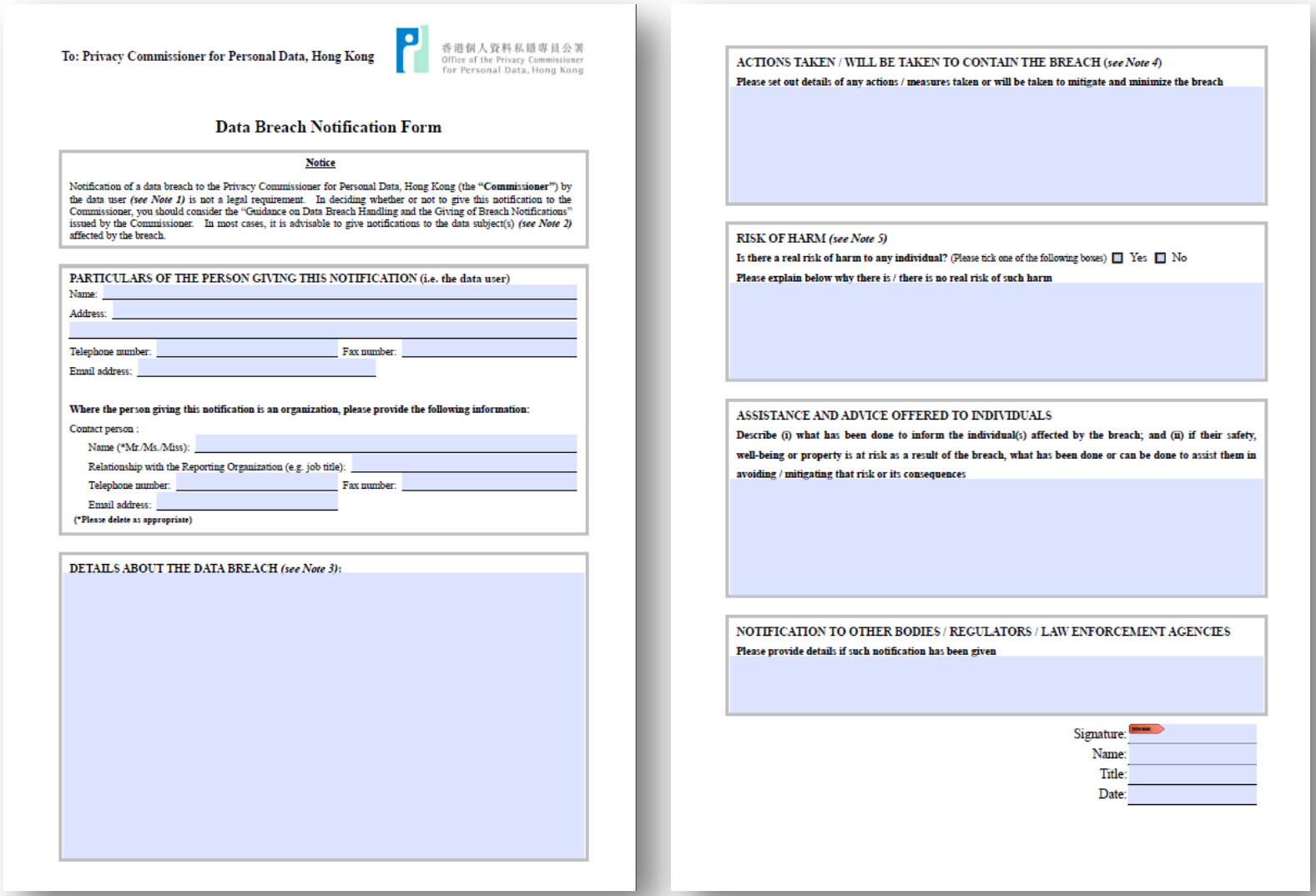
步驟1： 立即收集有關資料外洩事故的重要資料

資料使用者須立即收集下述資料：

1. 事故於何時發生？
2. 事故在哪裏發生？
3. 事故如何被發現及由誰人發現？
4. 事故的肇因是甚麼？
5. 涉及甚麼種類的個人資料及範圍有多大？
6. 受影響的資料當事人有多少？

[1] 「資料處理者」指代另一人處理個人資料及並不為該人本身目的而處理該資料的人。

Data Breach Notification Form



To: Privacy Commissioner for Personal Data, Hong Kong

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

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:

私 隱 管 理 系 統

Privacy Management Programme

From Compliance to *Accountability*

PMP – At a Glance

Part A: Baseline Fundamentals

1. Organisational Commitment		
a) Buy-in from the Top	b) Data Protection Officer/ Office	c) Reporting

2. Programme Controls		
a) Personal data inventory	b) Policies	c) Risk Assessment Tools
d) Training & Education	e) Breach Handling	f) Data Processor Management
g) Communication		

Part B: Ongoing Assessment and Revision

1. Oversight & Review Plan
2. Assess & Revise Programme Controls where necessary


Q
&
A


ngiyabonga
danke
謝謝
teşekkür ederim
спасибо
dank je
tapadh leat
thank you
gracias
hvala
mauruuru
mochchakkeram
bedankt
dziękuję
go raibh maith agat
sagolun
sukriya
kop khun krap
arigatō
takk
dakujem
obrigado
grazie
мерси
terima kasih
감사합니다
merci
ευχαριστώ