

**From Compliance  
to Accountability**



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

# How to Construct Comprehensive Privacy Management Programme

*31 October 2018*

*Natalie POON*

*Senior Personal Data Officer*

# Hacking



# Hacking

## 黑客入侵香港寬頻 失38萬客戶資料

有黑客盜取再  
更重系統就寬  
黑客入侵一個有已  
客戶個人資料，佔全  
4.3萬人的信用卡通  
科技罪案調查科跟進  
注信用的客戶資料，並  
有加密，香港寬頻僅  
個人資料被盜  
●去年1月一銀行發生電腦  
去年11月一銀行發生電腦  
去年1月一銀行發生電腦  
去年1月一銀行發生電腦

### 香港寬頻泄客戶資料 私隱專員：以全球營業額作罰則是大勢所趨

香港寬頻被黑客入侵客戶  
服務申請者紀錄，當中包括  
萬條信用卡資料，個人資料  
在香港寬頻通報前，已主要  
有遠近《個人資料（私隱）  
黃繼兒在商會節目提醒，並  
並聯絡銀行加強保安，以  
黃繼兒承認，香港有關私隱  
歐美一些國家已不斷修訂  
港未有類似懲罰機制。  
他認為，以全球營業額作罰  
阻嚇作用不大，他又表示，  
今次香港寬頻通報時間



# Loss of Storage Devices

South China Morning Post | HK CHINA ASIA WORLD COMMENT BUSINESS TECH LIFE CULTURE SPORT WEEK IN ASIA POST MAG STYLE TV

612 SHARES NOW READING Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive election

## Laptops containing 3.7 million Hong Kong voters' data stolen after chief executive election

Devices contained ID card numbers, addresses and mobile numbers

PUBLISHED : Tuesday, 28 March, 2017, 12:30am

UPDATED : Tuesday, 28 March, 2017, 1:42am

COMMENTS: 24

## 2017 Chief Executive Election of Administrative Region of the People's Republic of China



立場報  
STANDNEWS

選民資料電腦失竊 選舉事務處再解畫：無放入有鎖櫃 三日後方發現遺失

2017/4/10 — 21:56  
Like 333 f 8+ 5



要聞港聞 2016年09月04日 港大內科遺失3,675病人資料

## 港大內科遺失3,675病人資料

8,434



## Gov't admits it lost 2 computers containing details of 46 people during 2016 census

3 April 2017 15:23 · Eason Tong · 2 min read

The Hong Kong government has admitted that it lost two tablet computers containing the details of 12 households – 46 people – during last summer's census.

The Census and Statistics Department reported the missing devices to the police last summer. But it only revealed the matter to local media on Tuesday night, days after the Registration and Electoral Office announced that it lost two laptops containing the personal information of all registered voters.



盜。資料圖

院的手提電腦在上周四懷疑被盜，人姓名、身份證號碼、電話號碼、電腦需密碼登入，但只有901名病人，並向受影響病人致歉。有該系加上瑪麗正值重建，不排除因此

## HK

24h Reservation Hotline	Mon-Sun
+852 3916 3666	Hong Kong
+86 950715	Mainland China
+0080 1853033	Taiwan
+61 29009 7988	Australia
+64 9913 4177	New Zealand
+1 855 393 3880	U.S
Flight Status Enquiry	Mon-Sun
+852 3713 1388	0900-2200

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

# Emails Missent



## 大家樂泄近11萬會員資料 電郵附私隱誤傳一顧客 事發6日方通報





# Inadvertent Disclosure of Personal Data by Email

港聞

2017年4月12日 星期三

何郭佩珍中學電郵泄學生及家長資料 校長致歉：教B

## 何郭佩珍中學電郵泄學生及家長資料 校長致歉：教師一時失誤 危機處理小組 組跟進 (12:33)

8+ f 讚好 96

A+ A- 圖 鏈 郵 印



圖2-1 - (明報製圖 / Google街景圖片)

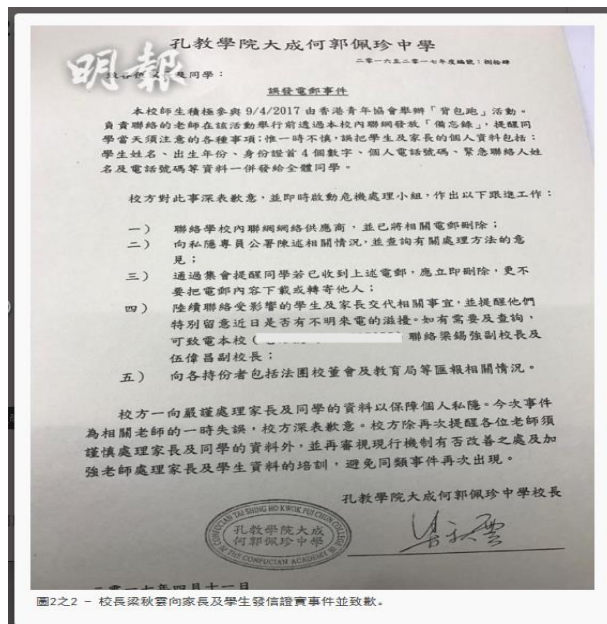


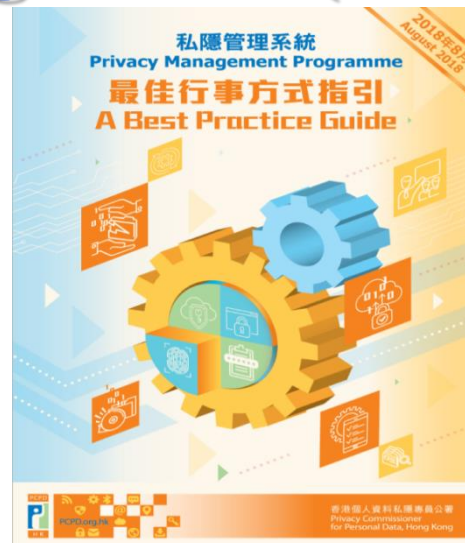
圖2-2 - 校長梁秋雲向家長及學生發信證實事件並致歉。

From Compliance... 由符規

To 躍升為問責  
Accountability



# Privacy Management Programme (PMP)





# Agenda

## Part I

What is Privacy Management Programme (PMP)

## Part II

How to develop your own PMP

# Part I

# What is PMP



# Hong Kong – Privacy Management Programme



Initiated by the Hong Kong  
Privacy Commissioner



Corporate governance  
responsibilities



Privacy risk  
management



A paradigm  
shift



Top-down business  
imperative



Data protection policies &  
procedures in place



Not a legal requirement



# Paradigm Shift

*From Compliance  
to Accountability*

## Compliance Approach

- **Passive**
- **Reactive**
- **Remedial**
- **Problem-based**
- **Handled by compliance team**
- **Minimum legal requirement**
- **Bottom-up**



## Accountability Approach

- **Active**
- **Proactive**
- **Preventive**
- **Based on customer expectation**
- **Directed by top-management**
- **Reputation building**
- **Top-down**

12

# Accountability

Guidelines on the  
Protection of Privacy  
and Transborder  
Flows of Personal Data



1980

2000



PIPEDA  
Principle 1:  
Accountability

APEC Privacy  
Framework -  
Principle 9:  
Accountability



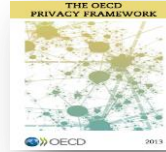
2005

2010



Article 29 Data  
Protection  
Working Party  
Opinion 3/2010 on the  
Principle of  
Accountability

OECD  
Revised  
Guidelines



2013

2014



HK: Privacy  
Management  
Programme  
Best Practice  
Guide

Australia:  
Privacy  
Management  
Framework



2015

2016



EU: General  
Data Protection  
Regulation

Source: adopted from  
[https://www.pcpd.org.hk/pmp/files/getting\\_to\\_accountability\\_01092015.pdf](https://www.pcpd.org.hk/pmp/files/getting_to_accountability_01092015.pdf)

13

PCPD

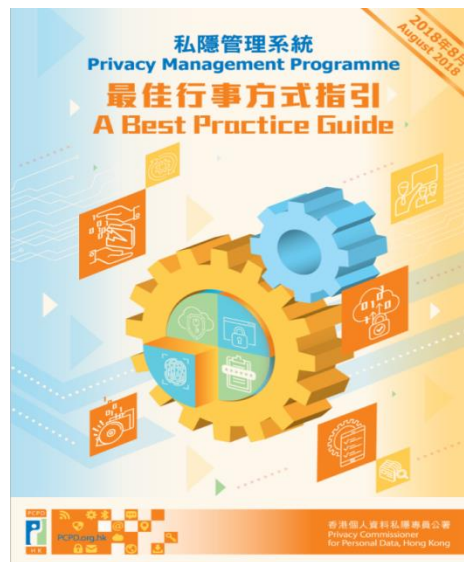
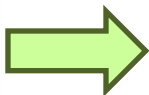
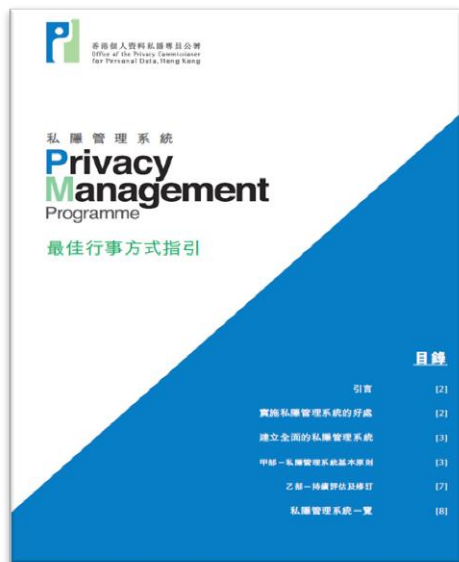


HK



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

# PMP: A Best Practice Guide



[https://www.pcpd.org.hk/english/resources\\_centre/publications/files/PMP\\_guide\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/PMP_guide_e.pdf)

A revised Best Practice Guide is issued in August 2018

14



# The Best Practice Guide **does not...**

Provide a “one-size-fits-all” solution

Provide direct guidance for compliance with specific provisions of the Ordinance

N

O

T

Constitute a Code of Practice under s.12 of the Ordinance

Impose prescriptive obligations

15

# The Benefits of implementing a PMP

1. You understand how privacy and data protection fit in to your overall business strategy
2. There is a clear understanding of what data is held, where it is and who has access to it
3. You know how well you are protecting the data, and where you are not
4. The risks introduced to the data by third parties are well understood and managed
5. The data is being used for the purpose that you have committed to, and nothing more
6. Minimise the risks of data breaches



# Why Privacy Management Programme



17



# GDPR Accountability vs. PMP

GDPR Requirements	PMP Components
Implement technical and organisational measure to ensure compliance [Art 24]	Seven Programme Controls
Maintain records of processing activities [Art 30]	Programme Controls (a) & (b) – Personal Data Inventory & Policies
Mandatory data breach notification [Arts 33-34]	Programme Control (e) – Breach Handling
Adopt data protection by design and by default [Art 25]	Programme Control (c) – Risk Assessment Tools
Conduct data protection impact assessment [Art 35]	
Designate data protection officer [Art 37 - 39]	Organisational Commitment (b) - Designate Data Protection Officer

18



# Participation in the PMP

## Media Statements

Date: 18 February 2014

## Major Organisations Pledge to Implement Privacy Management Programme to Protect Personal Data Privacy

(18 February 2014)

At a ceremony held today by the PCPD, the Hong Kong Special Administrative Region Government, together with twenty five companies from the insurance sector, nine companies from the telecommunications sector and five organisations from other sectors, all pledged to implement PMP.



PCPD



PCPD.org.hk

HK

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

# Consultancy Project on Implementation of PMP in Government

**PMP  
Training**



**Consultant engaged to  
facilitate bureaux  
/departments to  
implement PMP**



**PMP Manual**



**Advice  
provided by the PCPD**

20

PCPD



H K



[PCPD.org.hk](http://PCPD.org.hk)

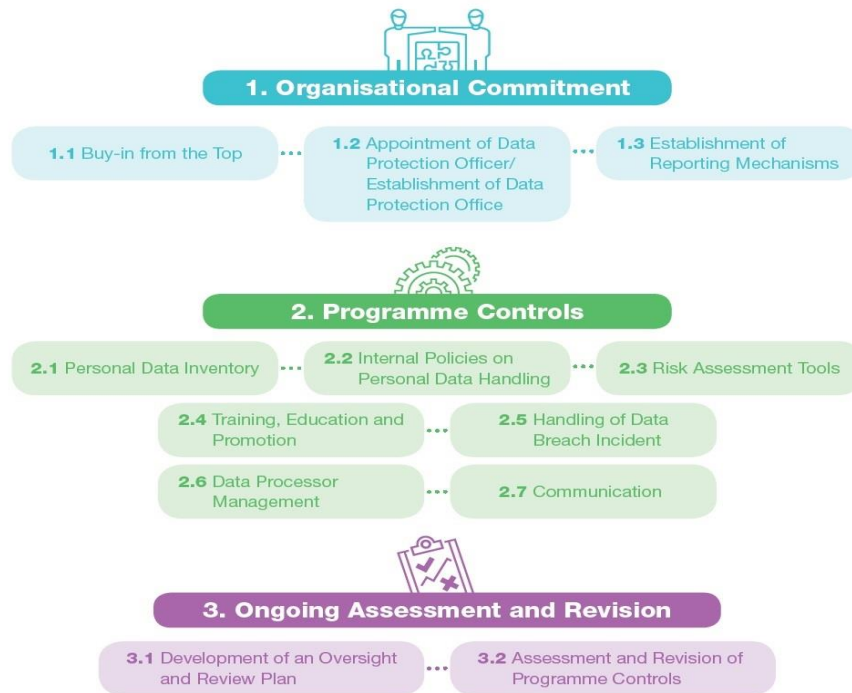
香港個人資料私隱專員公署  
Privacy Commissioner  
for Personal Data, Hong Kong

# PCPD's PMP

**We will do the same**



# Components of a PMP



# Components of a PMP Baseline Fundamentals



# Organisational Commitment

- Aim to foster a privacy respecting culture
- Range from a governance structure to practical procedures, and means to ensure the procedures are followed

# Organisational Commitment:

## 1.1) Buy-in from the Top

- Top management should:
  - endorse the PMP
  - appoint Data Protection Officer(s) (“**DPO**”)
  - allocate sufficient budget and manpower for implementation
  - actively engage in the review and assessment process

# Organisational Commitment:

## 1.2) Data Protection Officer/Office

- Role
  - Establish and implement programme controls
  - Coordinate with other appropriate persons responsible for related disciplines and functions within the organisation
  - Be responsible for the ongoing assessment and revision of programme controls
  - Represent the organisation in the event of an enquiry, an inspection or an investigation by the Commissioner
  - Advocate personal data protection within the organisation itself

26



# Organisational Commitment:

## 1.2) Data Protection Officer/Office

- Be a senior staff member
- May or may not be a full-time job
- May be supported by dedicated staff (Data Protection Office)
- (for larger organisations) Ideal to have a data protection coordinator in each major department to assist the DPO in the implementation of the PMP
- Large organisation VS. small organisation

27

# Example - Data Protection Office

## Structure of Data Protection Office

See p.39 of the  
Best Practice  
Guide

Role	Staff who took up the role	
Data Protection Officer	General Manager (Administration Department)	
Personal Data Privacy Officer	Senior Manager (Administration Department)	
Departmental Coordinator	Department	Staff who took up the role
	Administration	Manager <sup>4</sup>
	Information Technology	Senior Manager
	Corporate Communications	Senior Manager
	Legal	Senior Manager
	Marketing	Senior Manager

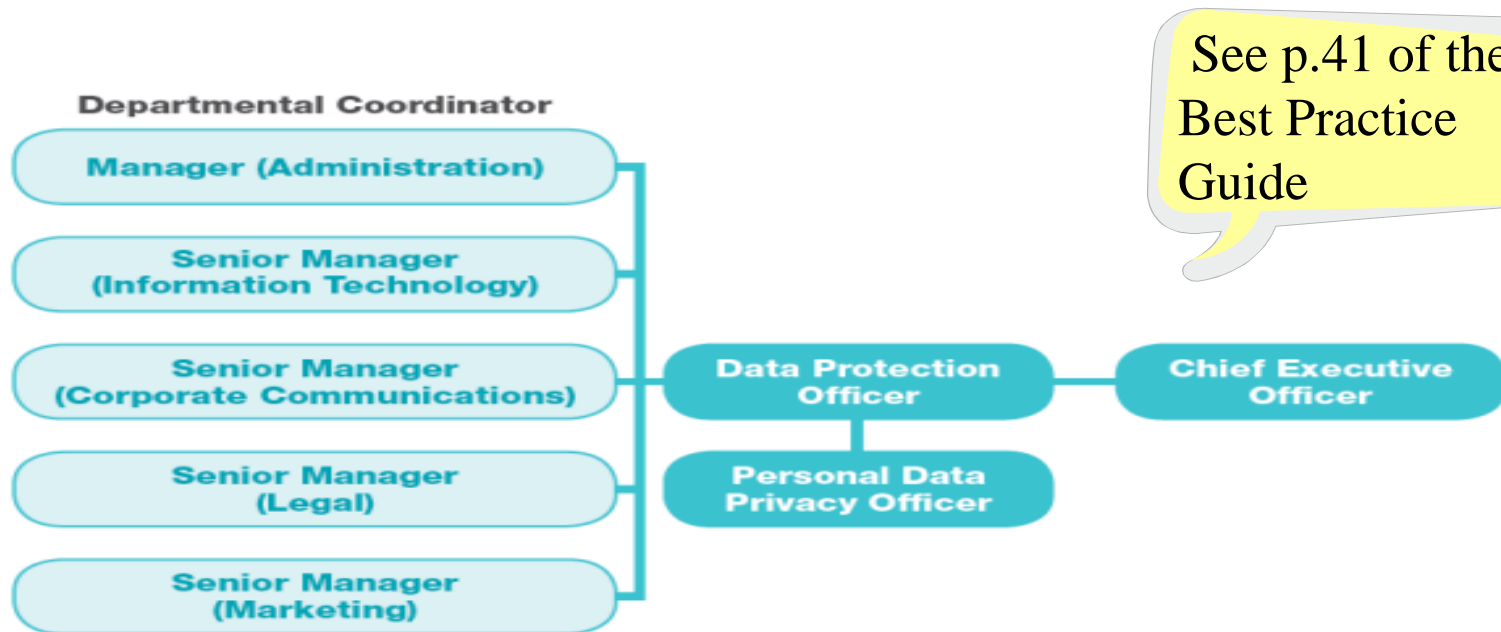
28

# Organisational Commitment:

## 1.3) Reporting

- Clear line of reporting effectively reaches top management (e.g.: Board of Directors)
- Assurance programme must be in place so that the day-to-day effectiveness and compliance issues can be reported
- Effectiveness and compliance of the PMP is communicated to top management regularly

# Example – Reporting Structure



# Components of a PMP Baseline Fundamentals





# Programme Controls

- Similar to the concept of other internal control procedures (e.g., procurement, recruitment)
- Assist organisations in bringing the principles and spirits of data protection into action
- Ensure & demonstrate compliance with the Ordinance

# Programme Controls:

## 2.1) Personal Data Inventory

An organisation should

- be clear about:
  - what kinds of personal data it holds
  - where the personal data is stored
  - why the personal data is collected
  - what are the limitations on the use of the personal data (e.g.: direct marketing)
  - what is the retention period
- properly document the above

33

# Programme Controls:

## 2.1) Personal Data Inventory

An organisation should

- Conduct Personal Data Inventory Review Exercise **annually**
- Establish clear procedures for inventory updating
  - time for updating
  - persons-in-charge
  - processes of updating and reviewing
  - persons responsible for filing the inventory

34

# Programme Controls: 2.1) Personal Data Inventory

## What kinds of personal data do you hold?

### CUSTOMERS

- Name
- Contact information (address, phone number, email, etc.)
- Purchase history
- Voice recording of telephone calls
- Etc.





### EMPLOYEES

- Name
- Gender
- Contact information
- HKID Card copy
- Salary
- Job title
- Medical benefits and MPF
- Appraisal

# Programme Controls: 2.1) Personal Data Inventory

Where the personal data is held?



-  Held by data processors?
-  Stored within the premises of the organisation?
-  Location of the storage / computer server?
-  Who is the owner (i.e. which department)?

36

## Programme Controls: 2.1) Personal Data Inventory

Why the personal data is collected?

Any use limitations?

### CUSTOMERS

- Provision of services
- Marketing
- Complaint/enquiries handling
- Processing application
- Open / Maintain / Terminate an account
- Conduct customer survey / research and perform statistical analysis
- Legal proceedings, including collecting overdue amounts

### EMPLOYEES

- Recruitment and HR management:
  - appointment
  - employment benefits
  - termination
  - performance appraisal
  - discipline
- Administration
- Tax

37



# Programme Controls: 2.1) Personal Data Inventory

## Benefits

- Decide the level of protection required for the data
  - e.g., higher security for sensitive data
- Determine the permitted uses of the data
  - e.g., can it be disclosed to 3<sup>rd</sup> parties?
- Facilitate compliance with data access requests
- Facilitate the impact assessment and remedy for data breach

### Alert:

- The Ordinance contains stringent requirements on **direct marketing**. It is important to have proper documentation about data subjects' consent to the use of their personal data for direct marketing purpose.

# Sample - Personal Data Inventory

Department	Administration	Marketing
Category of record	Personnel records	Membership records
Items of personal data contained in the record	Employees' personal data: - Name - HKID copy - Contact information (including address, mobile number and email address)	Members' personal data: - Name - Contact information (including address, mobile number and email address)
Means of collection of the data	Employee Information Form	Membership Application Form
Purpose of collection and use of the data	Handle employment-related matters	Handle matters related to provision of products and services to members
Retention period of the data	7 years after the employee has left the service	1 year after cancellation of membership by the member
Location for data storage	Physical: Filing cabinets in Personnel Record Room	Physical: Filing cabinets in Marketing Department Electronic: Network drive of Marketing Department

See  
p.44 of the Best  
Practice Guide

39

# Sample - Personal Data Inventory

Department	Administration	Marketing
<b>Disclosure of data to any third parties including data processors and the names and relevant details of third parties (Yes/No)</b>	No	Data will be transferred to service provider for telemarketing
<b>Possible location of transfer (e.g. cloud server location)</b>	N/A	Network drive of service provider
<b>Purpose of disclosing the data and whether the disclosure complies with the Ordinance</b>	N/A	Carry out telemarketing (consent has been obtained from data subjects)
<b>Date of return or destruction by the data processor (if applicable)</b>	N/A	Service provider will destroy the data within 7 days after expiry of contract
<b>Security measures adopted</b>	Filing cabinets are locked and the key is kept by Head of Personnel Department and Personnel Officer	Filing cabinets are locked and the key is kept by staff of Marketing Department. Marketing Department's network drive can only be accessed by staff of Marketing Department.

## Programme Controls: 2.1) Personal Data Inventory

### Data Protection Officer (DPO)

- To maintain an up-to-date inventory record
- Conduct Personal Data Inventory Review Exercise **annually**
  - Initiate the review exercise
  - Review and finalise the updated inventory submitted by Departmental Coordinator, seek clarification or further information when necessary
  - Ensure the updated personal data inventory covers all personal data held by organisation
  - File the updated inventory for record

41

# Programme Controls: 2.1) Personal Data Inventory

## Departmental Coordinator (DC)

- Update the inventory and keep track of retention period of personal data
- Ensure all types of records containing personal data are included in the inventory
- Identify any time-expired records during the review process
- Submit the updated inventory for DPO review & consolidation
- Ensure the justification and review the necessity of collecting personal information

# Programme Controls:

## 2.2) Internal Policies on Personal Data Handling

- Develop and document internal policies that address obligations under the Ordinance:
  - Policy for handling of customers' personal data
  - Human resources management policy (include employee monitoring)
  - Policy for outsourcing
  - IT and data security policy
  - CCTV policy
  - Policy for handling data access request from law enforcements, etc.
- Training or briefing to relevant employees
- Update and re-circulate the policies regularly

43

# Programme Controls:

## 2.2) Internal Policies on Personal Data Handling

### Cover the Six Data Protection Principles

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



資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的实际所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil 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



資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the 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.



# Example - Internal Policies on Personal Data Handling

## DPP1

Collection of personal data, including

- ▶ Handling of hotline enquiries
- ▶ Telephone recording
- ▶ CCTV monitoring
- ▶ Collection of Identity Card number and copy

See  
p.45 of the  
Best Practice  
Guide

## DPP2

Accuracy and retention of personal data

- ▶ Retention period of personal data related to employment (e.g. unsuccessful job applicants' personal data shall not be retained for a period longer than two years and former employees' personal data not more than seven years<sup>8</sup>)
- ▶ Retention period of data related to transactions with customers<sup>9</sup>

## DPP3

Use of personal data, including

- ▶ The requirements for consent
- ▶ Handling of requests from regulatory bodies, enforcement authorities and government departments for obtaining personal data

# Example - Internal Policies on Personal Data Handling

## DPP4

Security of personal data, including

- ▶ Security of physical documents containing personal data
- ▶ IT security (e.g. security measures for using portable devices containing personal data)
- ▶ Directing outsourced service provider to adopt necessary security measures when handling personal data

## DPP5

Transparency of organisations' personal data policies and practices

## DPP6

Steps for handling data access and data correction requests

## Section 35A of the Ordinance

- ▶ Actions to be taken before using personal data in direct marketing
- ▶ Steps for handling opt-out requests

# Programme Controls:

## 2.3) Risk Assessment Tools

- Periodic Risk Assessment
- Privacy Impact Assessment (PIA)



## 2.3.1 - Periodic Risk Assessment

- To ensure organisation's privacy policies and practices comply with the Ordinance
- To conduct **annually**



## 2.3.1 - Periodic Risk Assessment

Step 1

• DPO to inform DC to conduct periodic risk assessment and provide him/ her with the periodic risk assessment questionnaire

Step 2

• DCs to submit the completed periodic risk assessment questionnaire to DPO

Step 3

• DPO to review the questionnaire  
• If any non-compliant issue was found, DPO should inform relevant DC and obtain further information

Step 4

• DC to draw up mitigation measures for all identified risks in consultation with DPO to rectify the non-compliant areas

Step 5

• DPO to file the signed periodic risk assessment questionnaire for record

49

# Sample - Periodic Risk Assessment Questionnaire

Questions	Yes/No	Number	Further actions required
<b>A. New initiatives/projects developed or changes to existing activities involving personal data</b>			
1. Have any new initiatives/projects or changes to existing activities involving personal data been launched or developed in your department in the past 36 months, which involve the collection, use and processing of personal data (e.g. new personal data handling processes, launching of new systems, etc.) Please state the number of new initiative(s)/project(s) launched. If the answer is "Yes", please proceed to Q(2)-Q(4) below. If the answer is "No", please proceed to B.	( ) Yes ( ) No		See p.47 of the Best Practice Guide
2. Has all personal data involved in the new initiative(s)/project(s) or changes to existing activities been updated in the personal data inventory?	( ) Yes ( ) No		
3. Has privacy impact assessment (PIA) been conducted for the new initiative(s)/project(s) or changes to existing activities and submitted to the Data Protection Officer for review? Please also state the name(s) of the PIA(s) conducted.	( ) Yes ( ) No		

50

# Sample - Periodic Risk Assessment Questionnaire

4.	If a PIA has been conducted, are the content and result of the PIA still applicable? (i.e. Are there any new changes, new privacy risks and means to address those risks, which require updates on the PIA?)	<input type="checkbox"/> Yes <input type="checkbox"/> No		If no, please update the relevant documents and submit them to the Data Protection Officer.
<b>B. Data breach incidents</b>				
5.	Has any data breach incident occurred in the past 36 months in your department? If the answer is "Yes", please proceed to Q(6)-Q(7) below. If the answer is "No", please proceed to C.	<input type="checkbox"/> Yes <input type="checkbox"/> No		
6.	For each of the incidents, has a Data Breach Information Sheet been prepared and submitted to the Data Protection Officer?	<input type="checkbox"/> Yes <input type="checkbox"/> No		If no, please complete the Data Breach Information Sheet(s) and submit it to the Data Protection Officer.
7.	Has the data breach(es) been contained?	<input type="checkbox"/> Yes <input type="checkbox"/> No		

51



# Sample - Periodic Risk Assessment Questionnaire

C. Complaints received			
8.	Are there any complaints about your department's handling of personal data in the past 36 months?  If the answer is "Yes", please proceed to Q(9) below.  If the answer is "No", please proceed to D.	( ) Yes ( ) No	
9.	Were all relevant complaints reported to the Data Protection Officer? Please state the reference number of the complaints received.	( ) Yes ( ) No	If no, please report the complaints to the Data Protection Officer immediately.
D. New data processor			
10.	Has your department engaged any new data processor(s) to handle personal data in the past 36 months?  If the answer is "Yes", please proceed to Q(11) below.  If the answer is "No", please proceed to Q(12) below.	( ) Yes ( ) No	

52

# Sample - Periodic Risk Assessment Questionnaire

11. Has the Data Processor Review Checklist been completed and submitted to the Data Protection Officer?	( ) Yes ( ) No		If no, please complete the Data Processor Review Checklist and submit it to the Data Protection Officer.
<b>E. Data Retention Period</b>			
12. Has data disposal exercise been performed for all time-expired records within your department?	( ) Yes ( ) No		If no, please arrange for data disposal.

**Completed by  
(Departmental Coordinator)**

Signature \_\_\_\_\_  
Name \_\_\_\_\_  
Post \_\_\_\_\_  
Date \_\_\_\_\_

**Reviewed by  
(Data Protection Officer)**

Signature \_\_\_\_\_  
Name \_\_\_\_\_  
Post \_\_\_\_\_  
Date \_\_\_\_\_

## 2.3.2 - Privacy Impact Assessment

### When to conduct?

- Before introducing any new personal data process
- Before any *material change* to the data user's existing personal data process
- Where there is material change to regulatory requirements relating to personal data
- Periodically

## 2.3.2 - Privacy Impact Assessment

### Material change?

- Collection of new types of personal data (due to new services or products)
- Significant changes in the way personal data is used or disclosed (prescribed consent needed?)
- Significant change to the access right of a system containing personal data
- Outsourcing of data processing (include data storage)
- Outsourcing of IT management, etc.

55

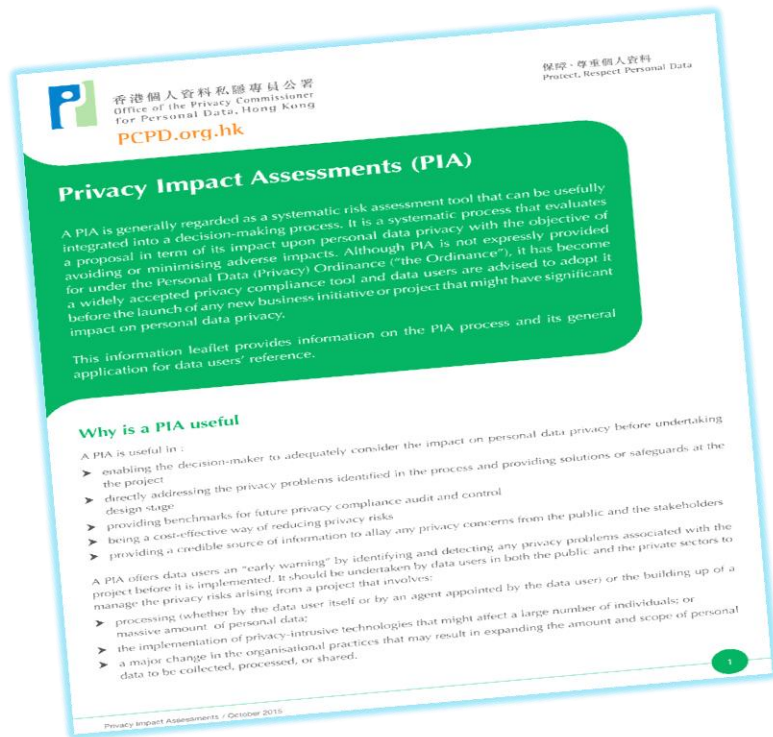
## 2.3.2 - Privacy Impact Assessment

An organisation should

- Develop internal policy to set out:
  - when Privacy Impact Assessment is required
  - what need to be done in the assessment
  - who are responsible for conducting and reviewing the assessment
- Upload the content of PIA on the organisation's website to enhance transparency



## 2.3.2 - Privacy Impact Assessment



*Information Leaflet on Privacy Impact Assessment issued by the PCPD*



## 2.3.2 - Privacy Impact Assessment

### Privacy Impact Assessment

- Evaluate a proposal in term of its impact upon personal data privacy

### Objective

- Avoid or minimise adverse impact

### Generally include:

- Data processing cycle analysis
- Privacy risks analysis (with ref. to the six Data Protection Principles)
- Avoiding or mitigating privacy risks
- Reporting and independent review



# Sample – PIA Questionnaire

Part A: Background information of the proposed change/project	
Project name	
Branch/Department	
Responsible officer (name & post)	
Expected date of implementation	
Description of the purpose of the personal data collection and the flow of handling personal data	See p.49 of the Best Practice Guide
Types of personal data to be collected (e.g. name, date of birth, Identity Card number, address, telephone number, etc.)	
Estimated number of data subjects from whom data is collected	
Will any data processor(s) be involved? If "yes", have contractual or other means been adopted to ensure that the data processor(s) has taken appropriate data security measures? If "no", please elaborate on the justification.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Will there be any cross-border transfer of personal data? If "yes", please specify the destination(s) and the purpose(s) of such cross-border transfer.	<input type="checkbox"/> Yes <input type="checkbox"/> No

59

# Sample – PIA Questionnaire

Part B: Privacy risks analysis		
Area	PIA Question	Answers by Branch/Division
<p>Data Protection Principle (DPP) 1 — Purpose and manner of collection of personal data</p> <ul style="list-style-type: none"> <li>▶ Personal data must be collected in a lawful and fair way, for a purpose directly related to a function or an activity of the data user.</li> <li>▶ 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.</li> <li>▶ Data collected should be necessary but not excessive.</li> </ul>	<p>Will the data subjects be informed of the purpose of collecting their personal data? If "no", please provide justifications.</p>	<p>( ) Yes ( ) No, _____</p>
	<p>Will the collection of personal data be on a minimum level (i.e. no excessive personal data is collected)?</p> <p>Please provide justifications on the collection of sensitive personal data below (including but not limited to):</p> <ul style="list-style-type: none"> <li>▶ Hong Kong Identity Card number and other personal identifier (e.g. passport number) <sup>13</sup></li> <li>▶ Biometric data (e.g. fingerprints) <sup>14</sup></li> </ul>	<p>( ) Yes ( ) No Justification on the collection of sensitive personal data: _____</p>
	<p>Will the data subjects be informed, on or before the collection of the personal data, of whether the supply of the personal data is voluntary or obligatory? If "no", please provide justifications.</p>	<p>( ) Yes ( ) No, _____</p>
	<p>Where it is obligatory for data subjects to supply the personal data, will the data subjects be informed of the consequence of not providing the personal data? If "yes", please elaborate. If "no", please provide justifications.</p>	<p>( ) Yes, _____ ( ) No, _____ ( ) Not applicable (it is completely voluntary for the data subjects to supply their personal data.)</p>
	<p>Will the personal data collected be transferred or disclosed to any third party?</p>	<p>( ) Yes ( ) No</p>
	<p>If the personal data is to be transferred to any third party or data processor, will the data subjects be informed of the classes of persons to whom their personal data may be transferred? If "no", please provide the reason.</p>	<p>( ) Yes ( ) No, _____ ( ) Not applicable (personal data collected will not be transferred or disclosed to any third party.)</p>

# Sample – PIA Questionnaire

Part B: Privacy risks analysis		
Area	PIA Question	Answers by Branch/Division
<p>DPP 2 — Accuracy and duration of retention of personal data</p> <p>► All practicable steps shall be taken to ensure personal data is accurate and is not kept longer than necessary to fulfil the purpose for which it was originally collected.</p>	<p>Will there be any measures in place to ensure accuracy of the personal data held? If "yes", please elaborate. If "no", please justify.</p> <p>What will be the retention period of the personal data? Please specify.</p> <p>Will there be any measures in place to ensure that personal data is not kept longer than necessary to fulfil the purpose of using the data? If yes, what are the measures? If no, please justify.</p>	<p>( ) Yes, _____</p> <p>( ) No, _____</p> <p>Retention period: _____</p> <p>( ) Yes</p> <p>( ) No, _____</p>
<p>DPP 3 — Use of personal data</p> <p>► Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless the data user obtains from the data subject voluntary and explicit consent to use the data for a new purpose.</p>	<p>Will personal data be used only for the original purpose stated in the Personal Information Collection Statement? If "no", what are the reasons.</p> <p>Where the personal data will be used for a new purpose, has explicit consent been obtained from the data subjects? If "no", please justify.</p> <p>Where personal data will be disclosed to a third party, will the third party be reminded of the use of the data and its responsibilities? If "yes", please elaborate. If no, please justify.</p> <p>Where personal data will be disclosed to a third party, is the personal data disclosed to third party only necessary but not excessive? If "no", please justify.</p>	<p>( ) Yes</p> <p>( ) No, _____</p> <p>( ) Not applicable (personal data will not be used for purposes other than the original purposes for which it is collected.)</p> <p>( ) Yes</p> <p>( ) No, _____</p> <p>( ) Not applicable (personal data collected will not be disclosed to a third party.)</p> <p>( ) Yes</p> <p>( ) No, _____</p> <p>( ) Not applicable (personal data of data subjects will not be disclosed to a third party.)</p>

# Sample – PIA Questionnaire

Part B: Privacy risks analysis		
Area	PIA Question	Answers by Branch/Division
<b>DPP 4 — Security of personal data</b> ▶ Data user needs to take all practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.	Will there be any safeguarding measures to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data? If "yes", please elaborate. If "no", please justify.	<input type="checkbox"/> Yes: _____ <input type="checkbox"/> No, _____
	Where data processor(s) will be engaged, will there be any contractual or other means to secure the personal data? If "yes", please elaborate. If "no", please state the reason.	<input type="checkbox"/> Yes, _____ <input type="checkbox"/> No, _____ <input type="checkbox"/> Not applicable (third party data processor will not be engaged.)
	Where data processor(s) will be engaged, is the personal data disclosed to data processor only necessary but not excessive? If "no", please justify.	<input type="checkbox"/> Yes <input type="checkbox"/> No, _____ <input type="checkbox"/> Not applicable (third party data processor will not be engaged.)
<b>DPP 5 — Openness of information</b> ▶ Data user must take all practicable steps to make known to the public its personal data policies and practices, types of personal data it holds and the main purposes for which it uses the data.	Is the existing Privacy Policy still applicable? If "no", please specify what update is needed.	<input type="checkbox"/> Yes <input type="checkbox"/> No: _____ _____
	Where there is a need to update the Privacy Policy, has the Data Protection Officer been informed and will the updated Privacy Policy be uploaded to the website before the implementation of the change/ the launch of the project? If "no", please explain. <b>[Note]</b>	<input type="checkbox"/> Yes <input type="checkbox"/> No, _____ <input type="checkbox"/> No update is required

# Sample – PIA Questionnaire

## *Points to Note on DPP 5*

If there is a need to update the Privacy Policy, the responsible officer should inform the DPO so that he can:

- ❖ make necessary amendments to the Privacy Policy
- ❖ upload the updated version onto the organisation's website

# Sample – PIA Questionnaire

<p>DPP 6 — Access to and correction of personal data</p> <p>► Data subject has the right to request access to his/her own personal data, and request the correction of the personal data if it is inaccurate.</p>	<p>Will the data subjects be informed of their right to access and correct their personal data? If "no", please justify.</p>	<p>( ) Yes ( ) No, _____</p>
	<p>Will the data subjects be informed of the post title and the address of the officer who is responsible for handling data access and correction requests? If "no", please justify.</p>	<p>( ) Yes ( ) No, _____</p>
<p><b>Part C: Potential risks and mitigation actions</b></p>		
<p><i>[For any privacy risks identified, please describe the means to address the risks.</i></p> <p><i>Based on the results of Part B, the responsible officer should assess the potential risks identified in relation to each of the DPPs, especially those areas with "No" as answers. These risk areas should be highlighted in the table below with the respective mitigating measures identified. For those risk areas where no mitigating measures could be identified, the responsible officer should consult the Branch/Department Head and the Data Protection Officer to assess the impact and whether the organisation could bear such risk.]</i></p>		
<p>Potential risks identified</p>		
<p>Mitigation measures</p>		

**Completed by  
(Departmental Coordinator)**

Signature \_\_\_\_\_  
 Name \_\_\_\_\_  
 Post \_\_\_\_\_  
 Date \_\_\_\_\_

**Reviewed by  
(Data Protection Officer)**

Signature \_\_\_\_\_  
 Name \_\_\_\_\_  
 Post \_\_\_\_\_  
 Date \_\_\_\_\_

## 2.3.2 - Privacy Impact Assessment

### Resources

- Information Commissioner's Office (UK) – **Conducting privacy impact assessments code of practice** (February 2014)  
<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>
- Office of the Australian Information Commissioner – **Guide to undertaking privacy impact assessments** (May 2014)  
<https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf>
- Privacy Commissioner (NZ) – **Privacy Impact Assessment Toolkit** (July 2015)  
<https://www.privacy.org.nz/news-and-publications/guidance-resources/privacy-impact-assessment/>
- PCPD's Information Leaflet – **Privacy Impact Assessments** (October 2015)  
[https://www.pcpd.org.hk/english/resources\\_centre/publications/files/InfoLeaflet\\_PIA\\_ENG\\_web.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf)
- EU Article 29 Working Party – **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679** (April 2017)  
[http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=50083](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

# Programme Controls:

## 2.4) Training and Education

- Tailored to specific needs of relevant employees (i.e. those handling personal data)
- Be given to new employees in its induction programme and periodically thereafter
- Cover organisation's policies and procedures
- Be delivered in an appropriate and effective manner
- Circulate essential information to relevant employees as soon as practical if an urgent need arises
- Monitor and keep records for attendance



66



# Example – Training and Education Activities

Area	Means / Channels
<b>The requirements of the Ordinance</b>	<ul style="list-style-type: none"><li>▶ Send employees to participate in the Privacy Commissioner's professional workshops, or arrange in-house training</li><li>▶ Provide essential training modules on the organisation's intranet</li><li>▶ Insert relevant modules in the organisation's monthly e-newsletters or training course on organisation policies</li></ul>
<b>The organisation's PMP</b>	<ul style="list-style-type: none"><li>▶ Explain relevant information to new employees in the organisation's induction programme, and circulate the information to all employees periodically (e.g. every six months)</li></ul>
<b>New/revised personal data privacy policies and guidelines</b>	<ul style="list-style-type: none"><li>▶ Circulate the information to all employees as soon as practical whenever the organisation issues new personal data privacy policies and guidelines, or makes amendments to current policies and guidelines</li></ul>
<b>Case sharing</b>	<ul style="list-style-type: none"><li>▶ Share with employees the complaint cases in relation to improper handling of personal data or data breaches, and educate them about the requirements of the Ordinance, proper way to handle the matters and how to prevent the recurrence of similar incidents</li></ul>
<b>Results of Privacy Impact Assessments</b>	<ul style="list-style-type: none"><li>▶ Share with employees the privacy risks identified in Privacy Impact Assessments and the mitigation measures taken</li></ul>

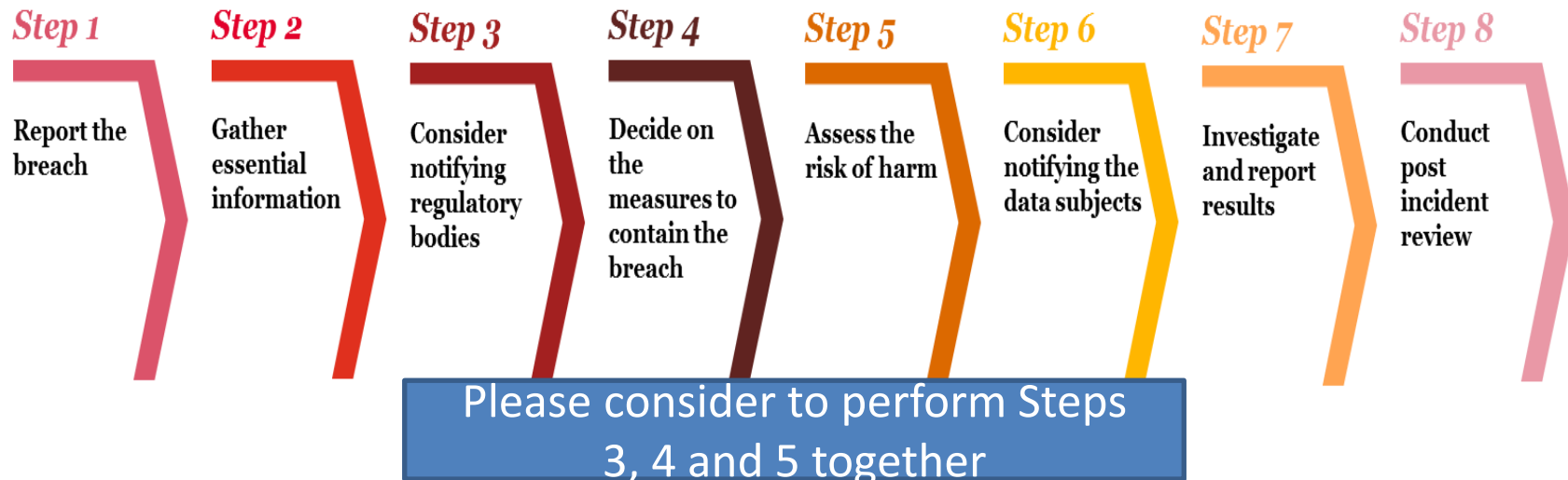
See p.54 of the Best Practice Guide

# Programme Controls: 2.5) Breach Handling



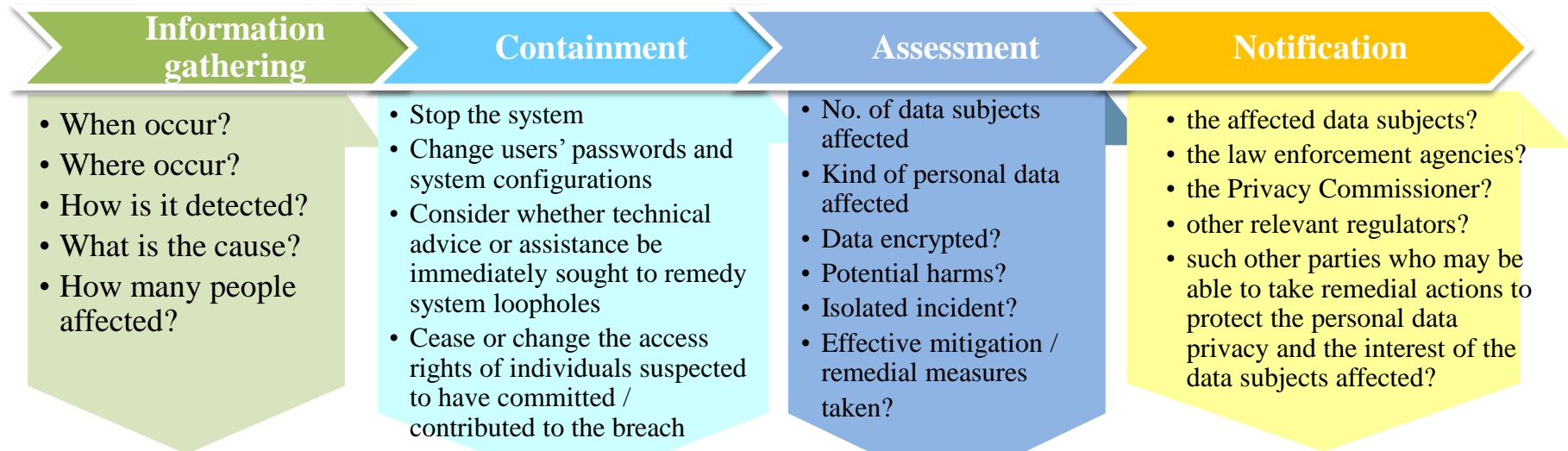
# Programme Controls: 2.5) Breach Handling

## Steps to be taken when handling data breaches



# Programme Controls: 2.5) Breach Handling

- Breach handling and notification procedure in place



Set out **procedures** and designate **officer(s)** to manage data breaches

PCPD's Guidance on Data Breach Handling and the Giving of Breach Notifications (Revised in October 2015)

[https://www.pcpd.org.hk/english/resources\\_centre/publications/files/DataBreachHandling2015\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf)

70

# Sample – Data Breach Information Sheet

BRANCH / DEPARTMENT	
Branch/Department	
(I) INFORMATION OF THE BREACH	
<i>(i) General information of the breach</i>	
Description of the breach	
Date and time of the breach	
Location of the breach (e.g. which office, which computer server, etc.)	
Date and time of discovering the breach	
How the breach is discovered (e.g. discovered during routine system checking, known after reported by media, etc.)	
Nature of the breach (e.g. loss of data, database is hacked, etc.)	
Cause of the breach	
<i>(ii) Impact of the breach</i>	
Types of data subjects affected (e.g. staff, customers, public, etc.)	
Estimated number of data subjects affected (Please state the respective number for each type of data subjects)	
Types of personal data affected (e.g. name, date of birth, Hong Kong Identity Card number, address, telephone number, etc.)	
Medium holding the affected personal data (e.g. physical folders, USB, etc.)	
If the personal data is held in electronic medium, is the data encrypted?	

See p.57 of the Best Practice Guide

# Sample – Data Breach Information Sheet

## (II) DATA BREACH NOTIFICATION TO REGULATORY BODIES

Are other regulatory bodies such as the Hong Kong Police Force or the office of the Privacy Commissioner for Personal Data, Hong Kong being notified of the data breach?

If **yes**, please provide the date and details of each notification given.

## (III) ACTIONS TAKEN/WILL BE TAKEN TO CONTAIN THE BREACH

Brief description of actions **taken** to contain the breach

Please evaluate the effectiveness of the abovementioned actions taken

Brief description of actions that **will be taken** to contain the breach

## (IV) RISK OF HARM

Please assess the potential harm to data subjects caused by the data breach and the extent of it

## (V) DATA BREACH NOTIFICATIONS TO DATA SUBJECTS AFFECTED

Dates and details of the data breach notifications issued to data subjects affected by the breach

If no data breach notification is issued/will be issued, please state the consideration



# Sample – Data Breach Information Sheet

## (VI) INVESTIGATION RESULTS

Cause(s) of the breach

## (VII) POST-INCIDENT REVIEW (To be completed by the Data Protection Officer)

Recommended improvement measures and the respective implementation date

Date to review the effectiveness of the abovementioned improvement measures

### Completed by (Departmental Coordinator)

Signature \_\_\_\_\_

Name \_\_\_\_\_

Post \_\_\_\_\_

Date \_\_\_\_\_

### Reviewed by (Data Protection Officer)

Signature \_\_\_\_\_

Name \_\_\_\_\_

Post \_\_\_\_\_

Date \_\_\_\_\_

# Programme Controls: 2.6) Data Processor Management

- Data processor:  
*“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”*
- Must adopt contractual or any other means to prevent:
  - personal data transferred to the data processor from being kept longer than is necessary for processing of the data (DPP2(3))
  - unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing (DPP4(2))
- A data users is liable to the act and practice of its data processor (S.65(2))

PCPD's Information leaflet: Outsourcing the Processing of Personal Data to Data Processors

[https://www.pcpd.org.hk/english/resources\\_centre/publications/files/dataprocessors\\_e.pdf](https://www.pcpd.org.hk/english/resources_centre/publications/files/dataprocessors_e.pdf)

74



# Programme Controls: 2.6) Data Processor Management



The types of obligations to be imposed on data processor include:



See p.59  
of the Best Practice  
Guide

75

# Sample – Data Processor Review Checklist

Part A: Background Information		
Branch/Department		
Name of data processor		
Purpose of engaging the data processor		
Brief description of personal data involved		
Date of engagement with the data processor		
Part B: Review of the organisation's management of data processors		
Questions	Yes/No (If no, please explain the reasons and justifications)	F
(1) Do the contractual terms cover the organisation's right to audit and inspect how the data processor handles and stores personal data?		
(2) Do the contractual terms cover the data processor's obligation to report immediately to the organisation for any signs of abnormalities, security breaches or loss of personal data?		
(3) Do the contractual terms cover the prohibition against any use or disclosure of the personal data by the data processor for a purpose other than the purpose for which the personal data is entrusted to it by the organisation?		
(4) Do the contractual terms cover the limitation on sub-contracting the service that it is engaged to provide?		
(5) Do the contractual terms cover the timely return, destruction or deletion of personal data by the data processor?		

See p.60 of the Best Practice Guide

76

PCPD



H K



PCPD.org.hk

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

# Sample – Data Processor Review Checklist

(6) Do the contractual terms cover the data processor's obligations to adopt security measures to protect the personal data entrusted to it and to comply with the Ordinance (please specify the security measures)?		
(7) Do the contractual terms cover the consequences for breach of the contract?		
(8) Is the Branch/Department satisfied that the data processor had followed the contractual obligations in respect of personal data protection? If "Yes", please elaborate.		
(9) If the answer to Q(8) above is "No", please specify the actions taken by the Branch/ Department?		
(10) Has the Branch/Division performed any audit and inspection on the data processor in the past 36 months (including surprise visit)? If the answer is "Yes", please state:  10.1 the date of the audit and inspection;		

# Sample – Data Processor Review Checklist

<p>10.2 any irregularities identified; and</p> <p>10.3 any remedial actions taken.</p> <p>If the answer is "No", please explain why an audit/inspection is not performed.</p>		
<p>(11) If audit and inspection were performed on the data processor this year, has the Branch/ Department identified any irregularities? If "Yes", please state the details and the improvement measures taken by the data processor.</p>		
<p>(12) Has there been any data breach incidents caused by the data processor? If "Yes", please provide the corresponding Data Breach Information Sheet as attachment.</p>		

**Completed by  
(Departmental Coordinator)**

Signature \_\_\_\_\_  
 Name \_\_\_\_\_  
 Post \_\_\_\_\_  
 Date \_\_\_\_\_

**Reviewed by  
(Data Protection Officer)**

Signature \_\_\_\_\_  
 Name \_\_\_\_\_  
 Post \_\_\_\_\_  
 Date \_\_\_\_\_

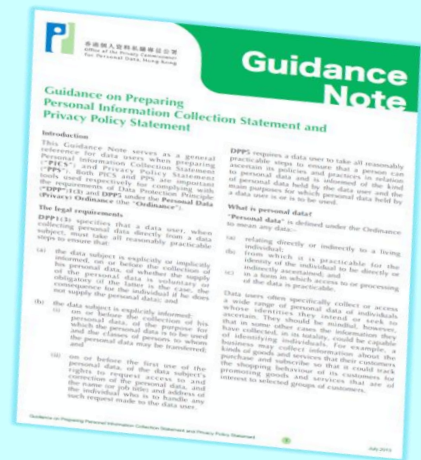
# Programme Controls: 2.7) Communication

Communication should be:

- readily available to customers, employees and other stakeholders
- clear, comprehensive, concise and easily understandable
- not simply reiteration of the Ordinance

Information to be covered:

- purpose of collection
- potential transferees
- retention period
- data security measures
- data subjects' right to access and correction of data
- contact person for privacy-related issues



# Components of a PMP



## 3. Ongoing Assessment and Revision

3.1 Development of an Oversight  
and Review Plan

...

3.2 Assessment and Revision of  
Programme Controls

# Ongoing Assessment and Revision

## 3.1) Develop an Oversight & Review Plan

- Developed by Data Protection Officer
- Endorsed by top management
- Cover-
  - the implementation of all Programme Controls
  - the review of all relevant policies and procedure
- Set out the assessment criteria and benchmarks for each Programme Control
- Designate the officer(s) responsible for conducting the review
- Carried out periodically (may also include ad hoc and surprise checks)

# Ongoing Assessment and Revision

## 3.1) Develop an Oversight & Review Plan

- Examples of action points to be included in an Oversight & Review Plan:
  - review and update personal data inventory
  - review and revise relevant policies and procedures
  - review and revise the risk assessment tools
  - review and update training materials and training plan
  - review and revise data processor contracts
  - test check the compliance with policies and procedures
  - test check the compliance by data processors
  - drill in data breach handling



# Sample – Oversight & Review Plan

Month	Oversight and review activities
Prepare the oversight and review plan	
Jan - Apr	<ul style="list-style-type: none"><li>▶ Update personal data inventory</li><li>▶ Review the organisation's data processor management</li><li>▶ Conduct periodic risk assessment</li><li>▶ Update training content and training plan</li></ul>
May - Jul	Assess the effectiveness of all PMP programme controls, and make corresponding amendments
Aug - Oct	Review and revise the PMP manual as well as other personal data privacy policies and guidelines
Nov	Circulate the PMP manual as well as other policies and guidelines related to personal data privacy to employees
Dec	Review the execution of the oversight and review plan, and prepare the plan for the next year

See p.64  
of the Best Practice  
Guide

# Ongoing Assessment and Revision

## 3.2) Assess & Revise Programme Controls

Backward looking (on compliance):

- How well has everyone adhered to the Programme Controls?
- Are the Programme Controls realistically achievable?
- Have the Programme Controls achieved their objectives?

Forward looking (on effectiveness):

- How to address the compliance issues (if any)?
- What are the areas of improvement?
- What are the suggested changes?

**Review report should be signed-off by DPO and submitted to top management.**



# Sample – PMP Review Document

Action	Completed/ Not completed	Date of last review/ update	Difficulties observed and proposed mitigation measures
(1) Update personal data inventory			
(2) Review of data processor management			
(3) Periodic risk assessments			
(4) Update training content and training plan			
(5) Review and revise the PMP manual, and other personal data privacy policies and guidelines			
(6) Circulate the PMP manual and other personal data privacy policies and guidelines to employees			
(7) Review the data breach handling mechanism			

See to p.65  
of the Best Practice  
Guide

## Part II

# How to develop your own PMP



86

# Key Steps

1

Structure  
the team  
(who)



2

Establish  
the  
framework  
(what)



3

Plan  
(how far)



4

Implement  
(when)



# 1. Structure the team

- Appoint a project lead (e.g. DPO) with sufficient privacy knowledge and authority to manage the project and assess the findings
- Ensure oversight by the top management through the project lead
- Involve HR, risk management, internal audit, compliance and IT personnel if necessary
- Seek outside privacy expertise if necessary

## 2. Establish the framework

Those developed by data protection authorities, e.g.:

- **Hong Kong**
  - Best Practice Guide on Privacy Management Programme
- **Canada**
  - Getting Accountability Right with a Privacy Management Program
- **Australia**
  - Privacy Management Framework



89

### 3. Plan

- Understand where you are, and decide where you want to be (Gap Analysis)
- Determine what are essential (core) and what are desirable (elective)
- Determine how to move from the current state to the desired state, and the time frame
- Determine who will carry out the change

Source: [http://www.pcpd.org.hk/privacyconference2014/files/9\\_neumann\\_presentation.pdf](http://www.pcpd.org.hk/privacyconference2014/files/9_neumann_presentation.pdf)



### 3. Plan: Core Activities

- Fundamental to the organisation for privacy and personal data management
- Identified by the Data Protection Officer as being mandatory
- Vary from one organisation to another:
  - Industry/sector (e.g.: banking; retail)
  - Size of organisation (e.g.: MNC; SME)
  - Mode of operation (e.g.: manual; computerised)
  - Type of personal data (e.g.: contact information; financial information)
- Examples: Review and update privacy policy regularly; maintain regular training and briefing to staff.

### 3. Plan: Elective Activities

- **Go beyond the minimum** for compliance and risk management
- Being elected to implement to further embed privacy throughout the organisation
- Examples:
  - Hold an annual data privacy day/week
  - Engage third party to conduct audit and assessment



92

# 3. Plan: What to implement

- Implement the core activities only?
- Implement core and elective activities?



# 4. Implement

- Put the activities in place
  - Allocate resources
  - Communicate the plan
  - Execute



Source:

[http://www.pcpd.org.hk/privacyconference2014/files/9\\_neumann\\_presentation.pdf](http://www.pcpd.org.hk/privacyconference2014/files/9_neumann_presentation.pdf)

94

## 4. Implement: ongoing review

- PMP – Not a one-off project
- Require ongoing monitoring, assessment and revision in order to stay effective and relevant



95

# Contact Us



## Copyright



This PowerPoint 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 PowerPoint, 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](https://creativecommons.org/licenses/by/4.0).

96

☐ Hotline

2827 2827

☐ Fax

2877 7026

☐ Website

[www.pcpd.org.hk](http://www.pcpd.org.hk)

☐ E-mail

[enquiry@pcpd.org.hk](mailto:enquiry@pcpd.org.hk)

☐ Address

1303, 13/F, Sunlight Tower,  
248 Queen's Road East,  
Wanchai, HK

PCPD



HK

[PCPD.org.hk](http://PCPD.org.hk)

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