University Privacy Campaign 2014

Personal Data Protection for internal IT Professionals

Henry Chang
FBCS, CITP, CEng, MIET, CISSP, CISM, CEH, CHFI, CIPT, CIPM
IT Advisor
Office of the Privacy Commissioner for Personal Data, Hong Kong
Jan 2015

Note: The contents herein are for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance ("the Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Privacy Commissioner for Personal Data ("the Commissioner") makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The contents herein will not affect the exercise of the functions and power conferred to the Commissioner under the Ordinance.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

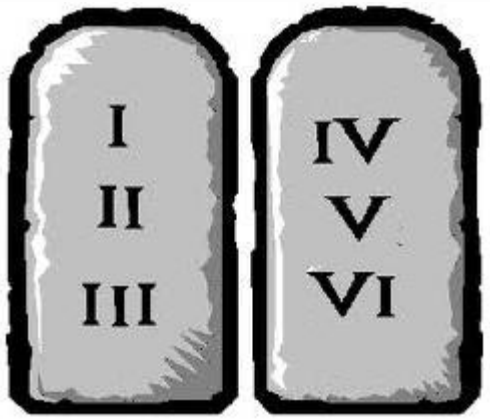
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Topics

1. Data Protection Principles
2. The CIA Principles
3. The Privacy by Design Approach
4. Direct marketing requirements
5. Common issues when managing Internet systems
6. Use of portable storage devices
7. Erasure and retention
8. Using clouds
9. Engaging data processors

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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



The Six Data Protection Principles

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Definition

Any data:

1. relating directly or indirectly to a living individual;

2. from which it is practicable for the identity of the individual to be directly or indirectly ascertained ; and

3. in a form in which access to or processing of the data is practicable.

Are these personal data?

a) Email addresses
b) IP addresses
c) cookies

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Data Protection Principles

1. Informed Consent
2. Protection
3. Transparency

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

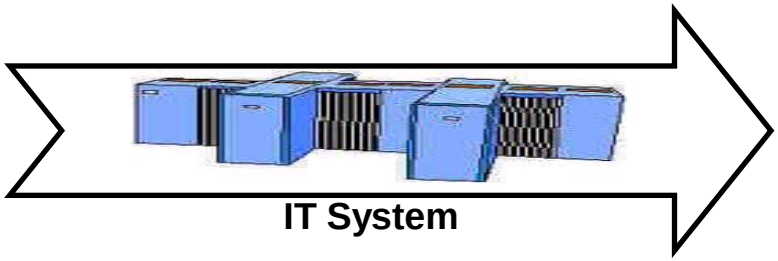
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Data Flow and Data Protection Principles (DPPs)

Personal Data Flow

Collection

Storage, Use or Processing



Retention/ Erasure

DPP 1 – Collection

DPP 3 – Use

DPP 2 – Accuracy and retention

DPP 4 – Security (IT and physical)

DPP 5 – Transparency

DPP 6 – Rights of access and correction

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Protection of Personal Data System
and
The CIA

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

C I A

For Personal Data Protection:
(Fair collection, Transparency, Need-to-know, right of access/correction)

For IT Security:
(Confidentiality, Integrity, Availability)

Confidentiality, Accountability, Integrity

Confidentiality, Integrity

For Personal Data System Protection:
(Confidentiality, Integrity, Accountability)

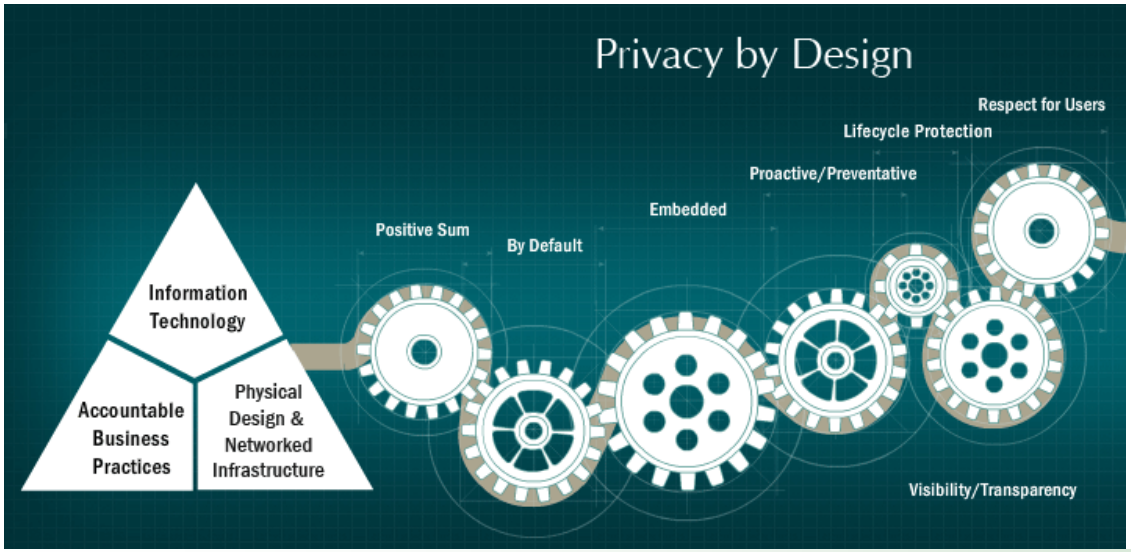
香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East, Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

Top-down Approach

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Privacy by Design



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Privacy by Design

Privacy by Design* is the philosophy of embedding privacy from the outset into the design specifications of accountable business processes, physical spaces, infrastructure and information technologies

*http://privacybydesign.ca/

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

The essence of Privacy by Design

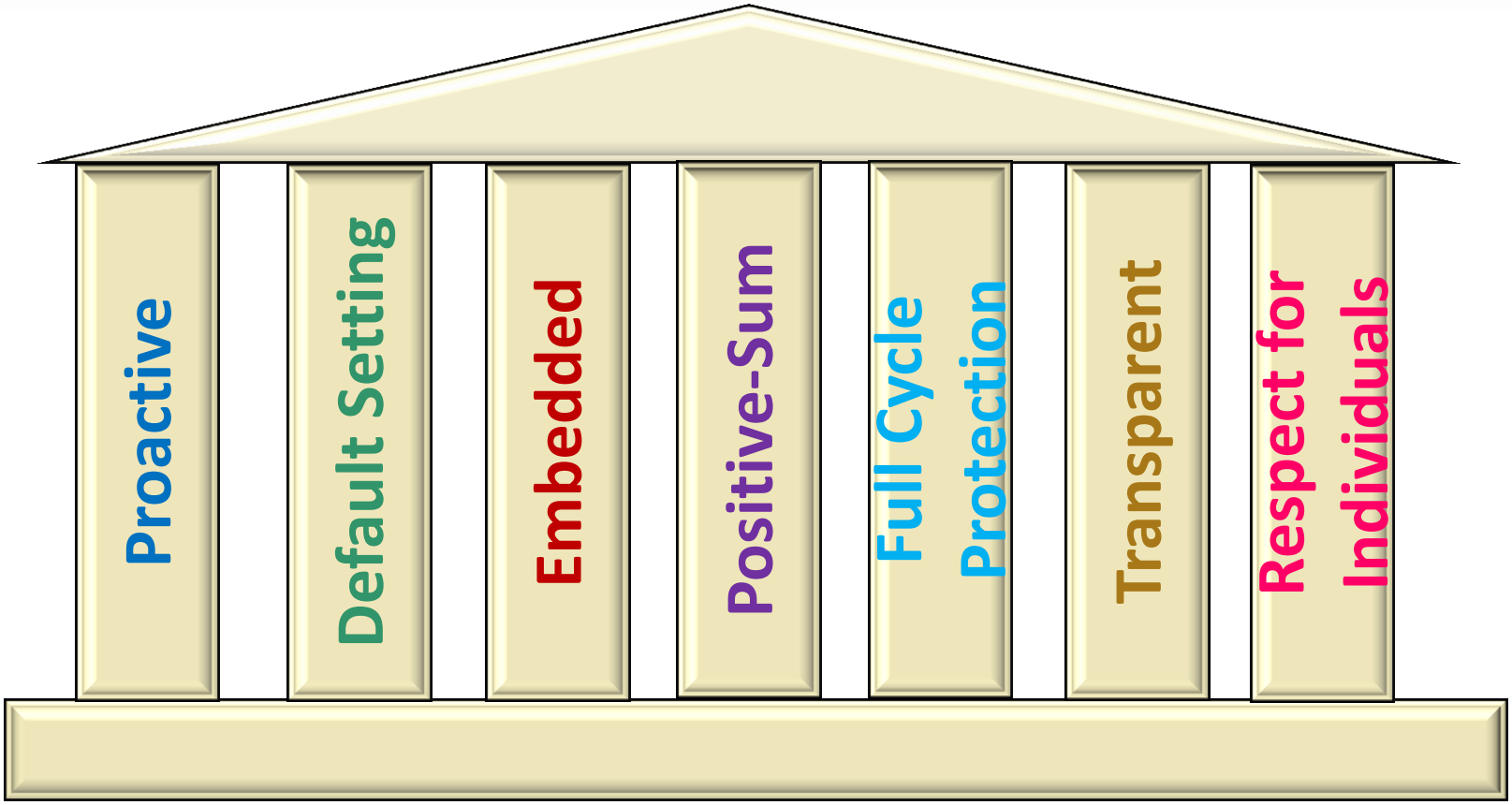
A clever person solves problem,

a wise person avoids it.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Privacy by Design Principles



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

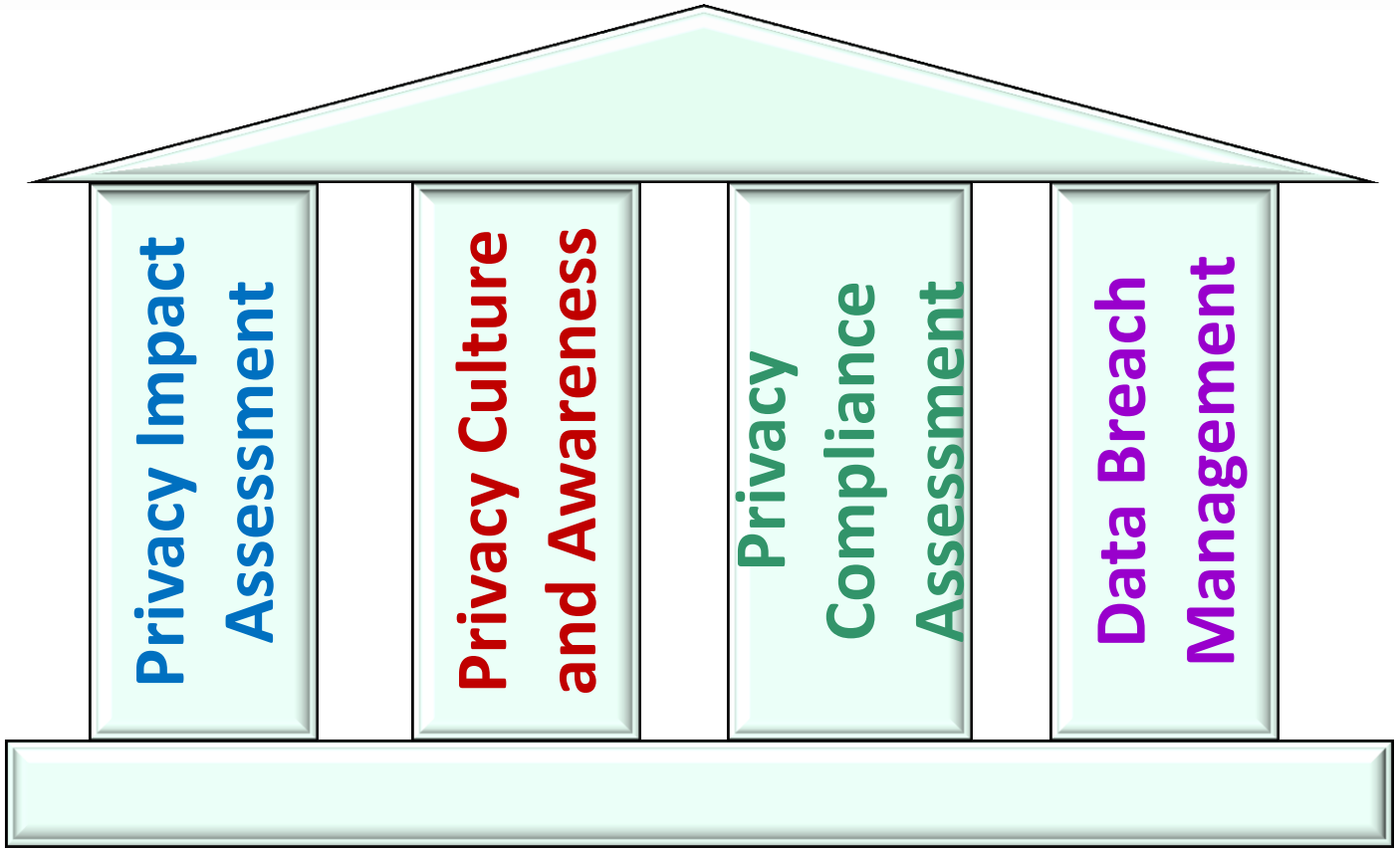
Privacy by Design Principles

1. Personal data protection should be proactive (not reactive) and preventive (not remedial) in nature;
2. Personal data privacy should be as the default setting;
3. Personal data privacy should be embedded into the design and not a bolt-on;
4. Personal data privacy design should be "win-win" and not a trade-off against functionality or security;
5. Personal data protection should cover the entire cycle of personal data flow from collection to erasure;
6. Personal data privacy design should be transparent to all stakeholders to allow for verification;
7. Personal data privacy design should be people-centric to address their concerns.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Privacy by Design Tools



香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Privacy by Design Tools

Privacy Impact Assessment

- A systematic evaluation of a proposal in its impact on personal data privacy with a view to avoiding or minimising adverse impacts.

Privacy Culture and Awareness

- Personal data privacy protection is not a silo compliance issue but a corporate culture that could differentiate an organisation.

Privacy Compliance Assessment

- A systematic assessment on the level of privacy compliance with the Ordinance and any established policies, guidelines and procedures.

Data Breach Management

- Data breach incidents need to be managed proactively and in a planned manner like DRP/BCP.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

The 'new' direct marketing provisions

*** Home > Resources Centre > Publications > Guidance Notes > Direct Marketing > New Guidance on Direct Marketing*

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Direct Marketing and Sections 35A – 35M

Part VI A: Use of personal data in direct marketing and provision of personal data for use in direct marketing

- Data subjects to be informed of the direct marketing intention and details; and

- consent (or 'no indication of objection') must be obtained from data subjects before direct marketing is to take place; or
- written consent (or 'no indication of objection') must be obtained from data subjects before personal data is to be transferred to others for direct marketing.

- if the data subject so requests, cease to so use those data without charge to the data subject.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Direct Marketing and Sections 35A – 35M

Part VI A: Exemptions (35B):

This Division does not apply in relation to the offering, or advertising of the availability, of -

a) social services run, subvented or subsidized by the Social Welfare Department;

b) health care services provided by the Hospital Authority or Department of Health; or

c) any other social or health care services which, if not provided, would be likely to cause serious harm to the physical or mental health of -

   i. the individual to whom the services are intended to be provided; or

   ii. any other individual.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Collecting and Using Personal Data through the Internet

*** Home > Resources Centre > Publications > Guidance Notes > Information and Communications Technology > Guidance for Data Users on the Collection and Use of Personal Data through the Internet*

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Collection and Use of Personal Data via the Internet

Common issues

- Identity of data users unclear
- Excessive collection
- Excessive disclosure
- Data leakage
  - Unclear requirements and responsibility for contractors
  - No segregation between production, testing and development environments
  - Weak access and password control
  - Lack of administrative control over encryption
  - Technical safeguards – three-tier, vulnerability test (don't forget app scanning), privacy-enhancing technologies
  - No 'predicable' URLs for information that should be protected by access control
  - No 'hidden'/unprotected file in webserver – if it is there, search engines will find it!
  - No HKID as password/shared secret!!
  - Maintenance files left on webservers
  - Check with Google hack!

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Portable Storage Devices

*** Home > Resources Centre > Publications > Guidance Notes > Information and Communications Technology > Guidance on the Use of Portable Storage Devices*

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Portable Storage Devices

- Top-down approach
  - Risk Assessment/Reconnaissance
    - Why, what, when, where , who, and how
  - Policy, Guidelines and Procedures
    - Given the specificity of PSDs, operational procedures are expected to ensure compliance

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Portable Storage Device

- Measures
  - Avoidance
    - How to minimise/limit the exposure/risk
  - Prevention
    - How to minimise/limit the damage
  - Detection
    - How to remind users of their exposure

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Portable Storage Devices

- Management
  - Staff awareness
  - Non-compliance consequence
  - Regular review and audit

- Technical Controls
  - If administrative measures fail…

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Erasure and Anonymisation

** *Home > Resources Centre > Publications > Guidance Notes > Information and Communications Technology > Guidance on Personal Data Erasure and Anonymisation*

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Erasure and Anonymisation

Personal Data Erasure (Top-Down Approach)

- **Retention Policy**
  - Related to Section 26 and DPP2(2)

- **Erasure Policy**
  - Related to Section 26, DPP2(2) and DPP4
  - "Practicable steps" to ensure data not kept longer than necessary
  - To Include Erasure Record Management
    - Erasure Record must not itself reveal erased personal data
  - To Include variants/copies of data and the disposal arrangement
  - Use 'fit for purpose' methods
  - Contractor control

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Erasure and Anonymisation

Anonymisation as an alternative

- Anonymisation ≠ De-identification
- Anonymisation in the eyes of data users and others
- Anonymised data should not be released/shared
- Anonymised data can become identifiable after further collection
- Anonymisation may not be possible
- The 'benefit vs risk' test

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Cloud Computing

*** Home > Resources Centre > Publications > Information Leaflets >Information and Communications Technology > Cloud Computing*

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Cloud Computing

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Bottom lines of engaging clouds

- Data users are responsible for the protection of personal data

- Outsourcing data processing does not mean outsourcing legal liability

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Cloud Characteristics of Particular Concern

- Rapid transborder data flow

- Rapid/Loose outsourcing arrangement

- Standardised contract

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Rapid transborder data movement

- Transborder data flow restriction on personal or related data
  - S. 33 of PDPO on transborder data flow is not in effect at the moment
  - Does your data subject have a reasonable expectation that their personal data collected by you (HK-based entity) are protected?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Rapid transborder data movement

- Comparable data protection laws?
  - No protection of personal data if stored in jurisdictions without data protection law
  - Data users are still liable under local law
  - How to fulfil data protection obligations to customers?
  - Do you know where the data is residing?
  - Can you tell your customers where their data is residing?
  - Does the cloud provider know where you data is residing?
  - Can you restrict the storage locations in which your data will reside?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Rapid transborder data movement

- Potential access by foreign law enforcement agencies
  - Can you tell your customers who these agencies may be?
  - Is this explicitly stated in your customer contract?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Rapid/Loose outsourcing arrangement

- Contractual obligation/relationship
  - Could the 2nd or even 3rd layer contractors be handling your data for you?
  - How do you know the obligations/standards you have put on the cloud provider have been extended to their contractors?
  - Do you have a direct contractual relationship with those who handle your data?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Rapid/Loose outsourcing arrangement

- Are those who operate on your data subjected to any regulation?
  - Would outsourcers be based in jurisdictions other than the location of the data centres?
  - Are they accustomed to data protection principles?
  - Can they be sanctioned if they failed to protection your personal data?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Standardised contract

- Can they meet the same security (or security requirements) as your internal setup?
  - You would not lower your IT security as a result of outsourcing, would you?
  - How can you impose the same level of security in a cloud contract?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Standardised contract

- Can you audit their security?
  - How do you know the expected level of security has been achieved?
  - Can you carry out security audit on the cloud provider? If you can, how would you do it?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Standardised contract

- Data breach management and notification obligation
  - Given the diverse jurisdictional and contractual relationship, can the cloud provider commit to a data breach management and notification system that meets your need?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Standardised contract

- Till death us do part…
  - At the end of the contract, if it does not work out or simply when you want data to be erased, can you be sure that the data will be securely erased or returned to you (or the equivalent protection)?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Cloud is just a form of outsourcing, so…

- Can the cloud provider unilaterally change the agreement?
- Agreement must allow data users to discharge their duties (such as data access and correction requests), particularly in the case of SaaS
- "Use limitation" to be added to the agreement
- Possible to use end-to-end encryption to protect personal data?

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Bottom lines

- Data users are responsible for the protection of personal data
- Outsourcing data processing does not mean outsourcing legal liability
- The amendments to DPP2 and DPP4 on ensuring data processors do not hold on to personal data longer than necessary and exercise reasonable practicable protection

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

ISO 27018 Code of practice for protection of PII in public clouds acting as PII processors

- Applicable 27002 controls
- Additional and specific controls

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Principle	Example of control
Policy compliance	CSP must always process PII in accordance with the service's stated policies that have been disclosed to customers.
End-users' access rights	CSP must offer tools that help customers comply with their data protection obligations to their own end-users, including allow end-users to access, correct and/or erase PII.
Purpose limitation	CSP cannot use PII for marketing or advertising without express consent of customer. Such consent should not be a condition for receiving the service.
Breach notification	CSP must notify customer of any unauthorised access to personal data or to processing equipment or facilities resulting in loss, disclosure or alteration of personal data.
Data deletion	CSP must have and implement policy for data retention and destruction after termination of a contract.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

Principle	Example of control
Geographic location of data	CSP must identify countries where data may be stored, and the names of any sub-processors.
Law enforcement requests	CSP must notify customer of legally binding law enforcement requests to disclose customer data, unless such notification is legally prohibited
Confidentiality	CSP must enter into confidentiality agreement with staff who have access to PII and provide appropriate staff training.
Encryption	CSP must encrypt PII that is transmitted over public data-transmission networks
Independent reviews	CSP must subject their service to independent information security reviews at planned intervals, and offer customers independent evidence that appropriate measures are in place to ensure compliance with CSP's policies and procedures.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Personal Data Protection in the Cloud

ISO 27018 CoP for PII protection in public cloud - the sliver bullet?

- Too new to say
- It is a Best Practice like ISO27002, not a Standard – assessment on actual controls may be required

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Engaging Data Processors

** *Home > Resources Centre > Publications > Information Leaflets > Others > Outsourcing the Processing of Personal Data to Data Processors*

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Engaging Data Processors

Definition of 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".

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Engaging Data Processors

Existing provisions:

DPP2:All practical steps must be taken to ensure that personal data is not kept longer than is necessary for the fulfilment of the purpose for which the data is or is to be used.

DPP4: All reasonably practicable steps shall be taken to ensure that personal data held by a data user are protected against unauthorised or accidental access, processing, erasure or other use.

s.65 about principle and agent's liability

New provisions:

DPP2 (3): If a data user engages a data processor, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary.

DPP4 (2): If a data user engages a data processor, 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.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Engaging Data Processors

Minimum considerations in contract:

- security measures or requirements
- timely return, destruction or deletion of the personal data when they are no longer required;
- prohibition against any use or disclosure of the personal data for other purposes;
- prohibition or restriction against sub-contracting;
- immediate reporting of any sign of abnormalities or security breaches;
- measures by data processor to ensure security and staff compliance are in place;
- data user's right to audit and inspection, or equivalent;
- consequences of violation of the contract.

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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

Engaging Data Processors

Other considerations :

- **Select reputable contractors that can ensure data security and/or with good track record;**
- **Use of contactors (and measures to protect personal data in such arrangement) should be transparent to data subjects;**
- **Clear instructions should be given to data processor in respect of the use, transmission, storage and destruction of the personal data, and a record kept for all the transfers;**
- **If data processors are not Hong Kong companies, how the contracts can be enforceable both in Hong Kong and in the location where the data processor are located;**
- **Whether testing by contractor should be carried out with production data and what the protection measures should be.**

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2827 2827 傳真 Fax (852) 2877 7026
電郵 Email enquiry@pcpd.org.hk 網址 Website www.pcpd.org.hk

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