

Legal Week's Corporate Counsel Forum 2016
Renaissance Harbour View Hotel
23 June 2016

Hong Kong Personal Data Protection Regulatory Framework – From Compliance to Accountability

Stephen Kai-yi Wong
Privacy Commissioner for Personal Data, Hong Kong

Disclaimer: The information provided in this PowerPoint 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 information set out in this PowerPoint. The contents provided will not affect the exercise of the functions and powers conferred to the Commissioner under the Ordinance.



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

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

PCPD.org.hk

PCPD New TV API

“Stay Smart. Mind Your Digital Footprint”



Stay Smart
Mind Your Digital Footprint

www.PCPD.org.hk

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

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

PCPD.org.hk

The Hong Kong Data Protection Law

The Personal Data (Privacy) Ordinance (the Ordinance)

- omnibus and comprehensive
 - covering the public (government) and private sectors
- referenced to OECD Privacy Guidelines and 1995 EU Directive
- enforced by an independent statutory regulatory body – the Privacy Commissioner for Personal Data

1	收集目的及方式 Collection Purpose Et 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傳給哪類人士。 收集的資料是有實際需要的，但不應乎過度。	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 Et 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成原來的目的實際所需。	Personal data is accurate and is not kept for a period 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、濫用、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 Et 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.

3



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

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

PCPD.org.hk

Amendments in 2012 upon Consultation

Key amendments
Direct Marketing (s.35A - M)
Outsourcing of personal data processing (DPP2(3) & 4(2))

New offence against disclosure of personal data obtained without data user's consent (s.64)

Legal assistance to affected individuals
Strengthening the Privacy Commissioner's enforcement power
New exemptions (e.g. legal proceedings etc.)



Regulatory Activities at A Glance

- investigation reports (complaint driven or self-initiated)
- specific consultations/surveys on topical issues
- comments and submissions on proposed legislation or major infrastructures that attract privacy concerns
- industry-specific privacy campaign
- publication of guidance materials (Code of Practice / Guidelines / Guidance Notes / Information Leaflets)
- professional compliance workshops
- data Protection Officers' Club
- support for small-medium enterprises
- online training platform and resources



5



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

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

PCPD.org.hk

Data Breach

- a data breach is generally understood to mean a suspected breach of security of personal data held by a data user, by exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use
- examples: (i) loss or leakage of personal data stored in notebook computers, USB flash drives, (ii) improper handling of personal data (e.g. improper disposal of personal data, sending to the wrong recipient or unauthorised access by employee), (iii) unauthorised access by hackers
- data breach notifications received
(*figure as at 31/3/2016)

Year	No. of Incidents
2015-2016*	104
2014-2015	66
2013-2014	76

6



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

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

PCPD.org.hk

Recent Data Leakage Incidents in HK

VTech Learning Lodge (electronic toy manufacturer)

Customers were allowed to download apps, games, e-books and other educational content from website to purchased products



Suspected leakage of data (profile of 5 million parents and over 6.6 million children)

SanrioTown

Members' personal data was stored in website



3.3 million members of its website made publicly accessible (involving names, email address, date of birth, encrypted password)

7



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

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

PCPD.org.hk

PCPD's Investigation

- obligation under Data Protection Principle 4 in Schedule 1 of the Ordinance.
- PCPD's compliance checks or investigation: huge impact and/or number of affected individuals
- enforcement notice to remedy and, if appropriate, prevent recurrence of the contravention

8



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

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

PCPD.org.hk

Data Breach: Regulatory Approach

lesson to learn from breach: to prevent recurrence

- Enhancement in the security and administrative measures in handling personal data (e.g. IT measures, internal privacy policies and guidelines)
- Control over access right (“need-to-know” and “need-to-access” basis)
- Proper categorization of data: “confidential”, “classified”, etc.
- strengthening of the monitoring and supervision mechanism (e.g. keep logs on access and use)
- Staff training
- Audit: a good privacy governance, preventing recurrence

“Guidance on Data Breach Handling and the Giving of Breach Notifications” : assist data users in handling data breaches, and to mitigate the loss and damage caused to the data subjects concerned

9



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

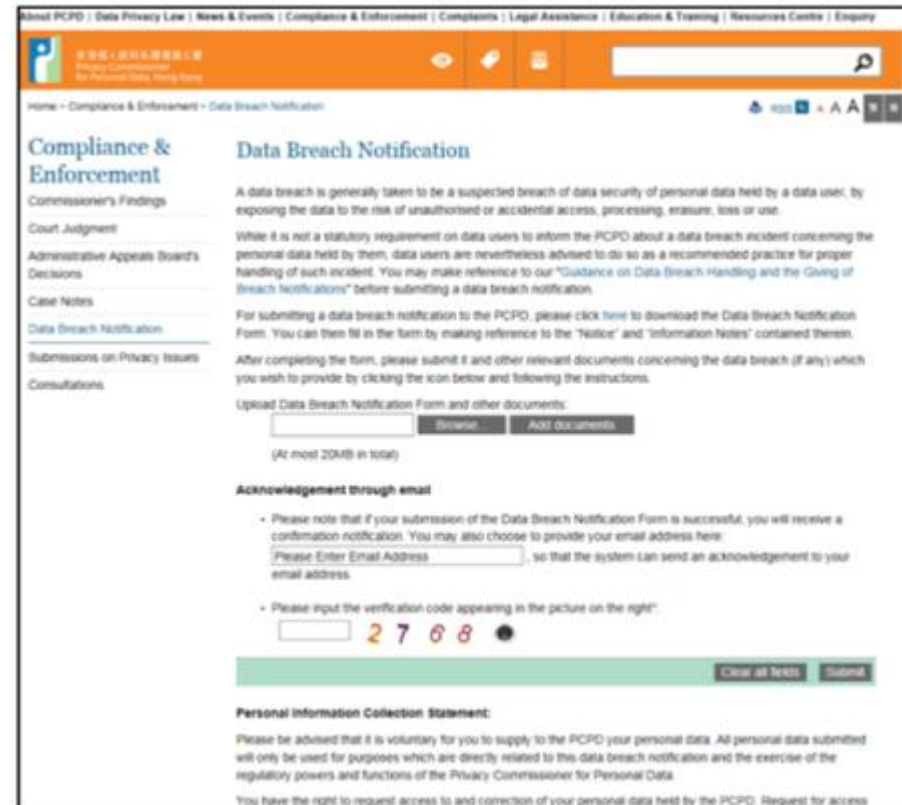
保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

Submission of Data Breach Notification



Data Breach Notification



10



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

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

PCPD.org.hk

Importance in Risk Management

research and consultation study on “Hong Kong Accountability Benchmarking Micro-Study” conducted in early 2015

purpose: to understand the current status of how privacy is being managed in Hong Kong

Focus on legal compliance requirements and specific Codes of Practices (HR Management) issued by PCPD

Invested heavily in measures related to technical and security measures, records retention, data privacy notices and policies, requirements for processors, and managing and responding to access requests

A higher percentage of organisations in Hong Kong implementing personal data inventory and data classification

Developing the privacy management programme in training and awareness; managing third-party risks; implementing privacy by design procedures; and testing incident and breach protocols



Privacy Management Programme (PMP)

Accountability Principle (OECD privacy principle)

a data user (controller) should be accountable for complying with measures which give effect to the data protection principles

Privacy Management Programme: a tool to assist building up accountability



*From Compliance
to Accountability*

12



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

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

PCPD.org.hk

Main Themes of a Privacy Management Programme

- “an accountable organisation must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management programme.”
- encourage organisations to embrace personal data privacy protection as part of their corporate governance responsibilities and apply it as a top-down business imperative throughout the organisation



13



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

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

PCPD.org.hk

Paradigm Shift

compliance approach:

- passive
- reactive
- remedial
- problem-based
- handled by legal/compliance
- minimum legal requirement
- bottom-up



accountability approach:

- active
- proactive
- preventative
- based on customer expectation
- directed by top-management
- reputation building
- top-down

14



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

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

PCPD.org.hk

Participation in the Privacy Management Programme

- participating sectors that pledged to implement PMP
 - Hong Kong Government
 - 25 insurance companies
 - 9 telecommunications companies
 - 5 organisations from other sectors

Privacy Management Programme



15



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

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

PCPD.org.hk

PMP Best Practice Guide - Fundamental Principles

three top-down management commitments:

**1. top-management
commitment and
buy-in**

**2. setting up of a
dedicated data
protection office or
officer**

**3. establishing
reporting and
oversight
mechanism for the
privacy
management
programme**

16



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

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

PCPD.org.hk

PMP Best Practice Guide - Fundamental Principles

seven practical programme controls:

1. recording and maintaining personal data inventory

2. establishing and maintaining data protection and privacy policies

3. developing risk assessment tools (e.g. privacy impact assessment)

4. developing and maintaining training plan for all relevant staff

5. establishing workable breach handling and notification procedures (e.g. data breach notification)

6. establishing and monitoring data processor engagement mechanism

7. establishing communication so that policies and practice are made known to all stakeholders

17



PMP Best Practice Guide - Fundamental Principles

two review processes:

1. the development of an oversight review plan to check for compliance and effectiveness of the privacy management programme

2. the execution of the oversight review plan making sure that any recommendations are followed through.

Part B
Ongoing Assessment and Revision

Oversight & Review Plan

- Develop an oversight and review plan

Data Protection Officer or Data Protection Office should develop an oversight and review plan on a periodic basis that sets out how the effectiveness of the organisation's programme controls will be monitored and assessed.

Assess & Revise Programme Controls Where Necessary

- Update personal data inventory
- Revise policies
- Treat risk assessment tools as evergreen
- Update training and education
- Adapt breach and incident response protocols
- Fine-tune data processor management

18



Consultancy on Implementing PMP in the Public Sector

November 2015 - to facilitate three HK Government bureaux/departments to implement PMP



- deliverables (toolkits and training) will be beneficial to organisations (public or private) implementing PMP



19

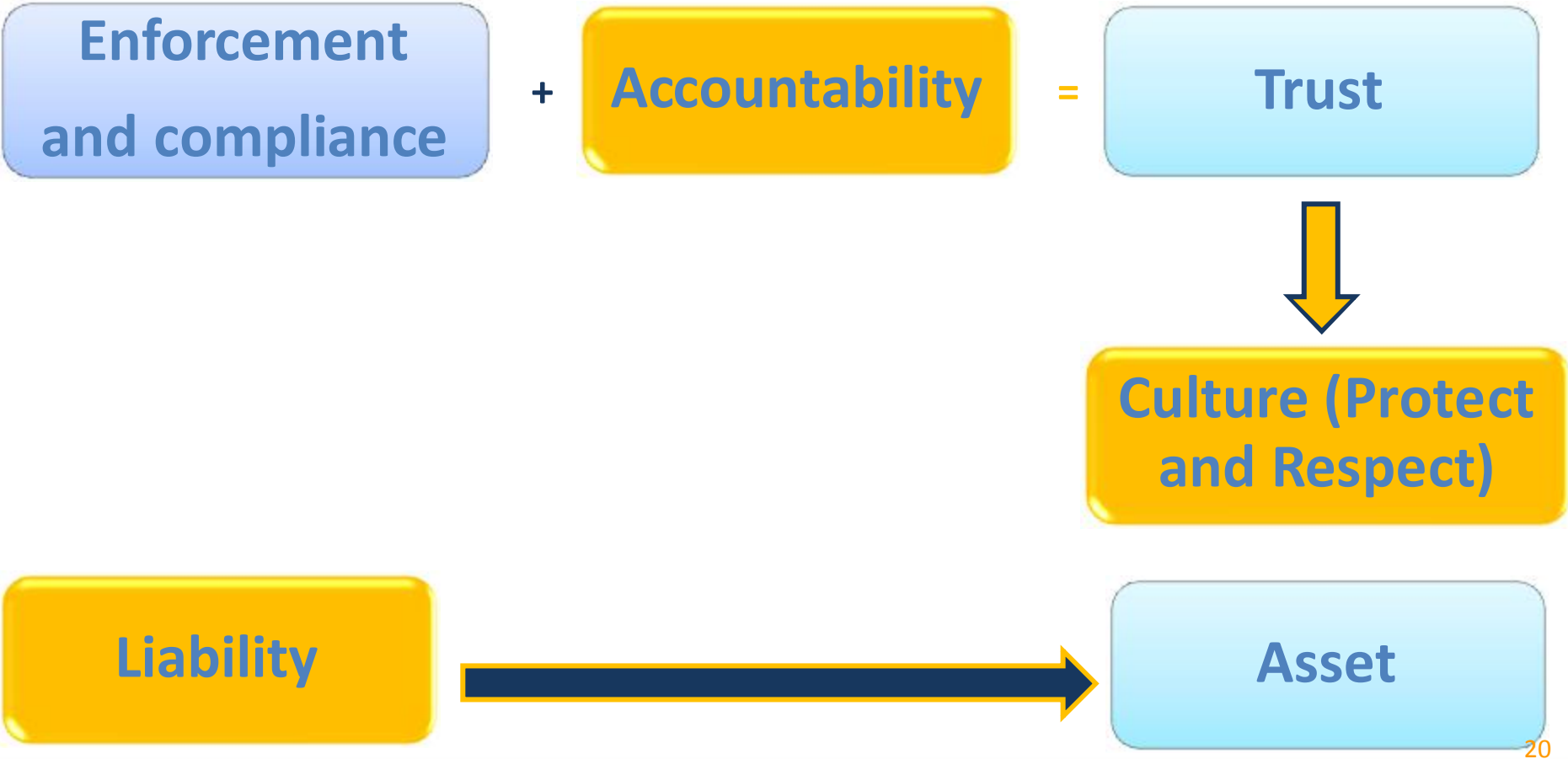


香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

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

PCPD.org.hk

Effect of Paradigm Shift



20



Buy-in From the Top

Example: Octopus

“Our Rule of Thumb

Organisational commitment – top-down directives and bottom-up processes

*We need to do **not just legal, but what is right**”*

Presentation by Mr Sunny CHEUNG, CEO, Octopus Holdings Limited, Hong Kong (2014)

21



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

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

PCPD.org.hk

Tips for In-house Counsel

keep abreast with new development
(PCPD's online resources, Data Protection Officer's Club)

prepare organisation to meet new changes
through risk assessments, protocols and policies

secure the buy-in from top-management

build a culture within organisation to protect privacy

oversight and review

22



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

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

PCPD.org.hk

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



Contact Us



- ☐ Hotline - 2827 2827
- ☐ Fax - 2877 7026
- ☐ Website - www.pcpd.org.hk
- ☐ E-mail - enquiry@pcpd.org.hk
- ☐ Address - 12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, HK

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.





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

PCPD.org.hk

