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

PCPD New TV API
“Stay Smart. Mind Your Digital Footprint”

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

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

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

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)

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

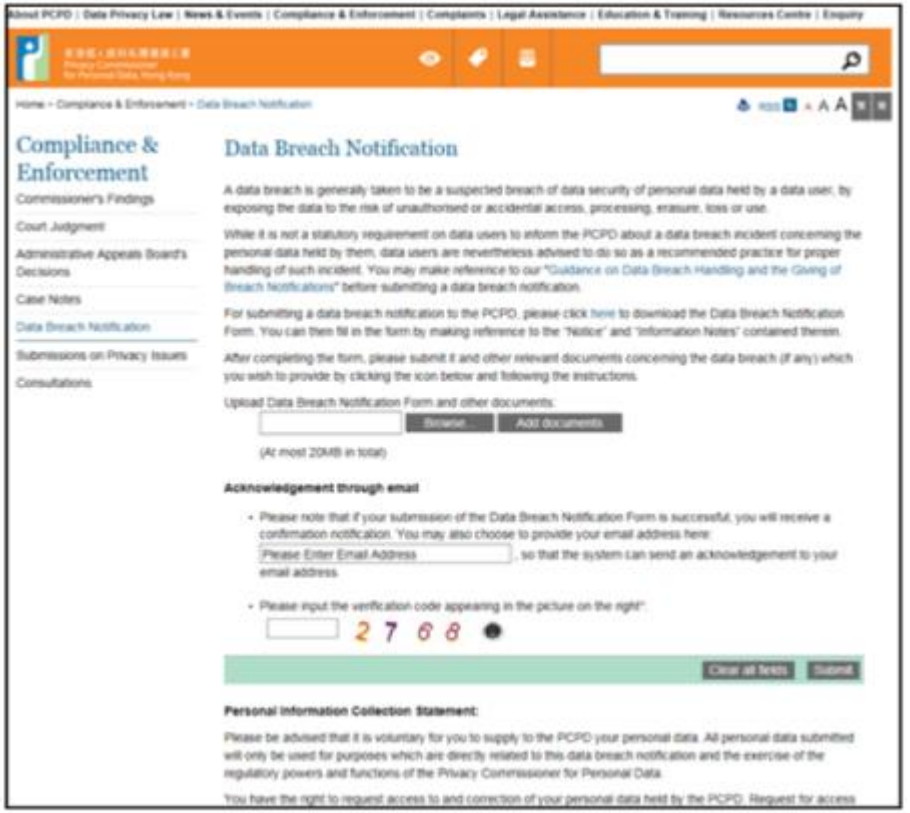
Data Breach: Regulatory Approach

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

Submission of Data Breach Notification



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

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

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

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

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**

PMP Best Practice Guide - Fundamental Principles

seven practical programme controls:

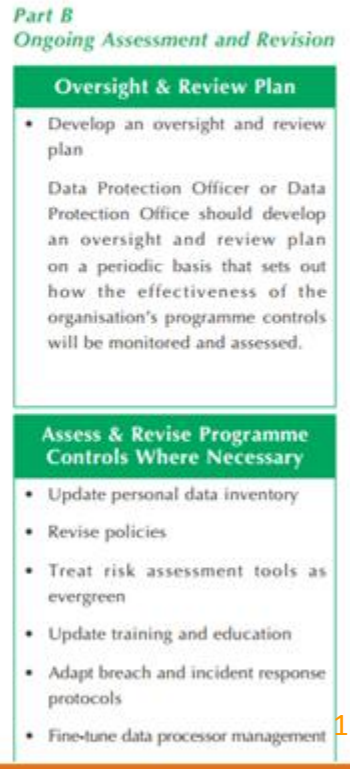
1. recording and maintaining personal data inventory
2. establishing and maintaining data protection and privacy policies
3. developing risk assessment tools (e.g. privacy impact assessment)
4. developing and maintaining training plan for all relevant staff
5. establishing workable breach handling and 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

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

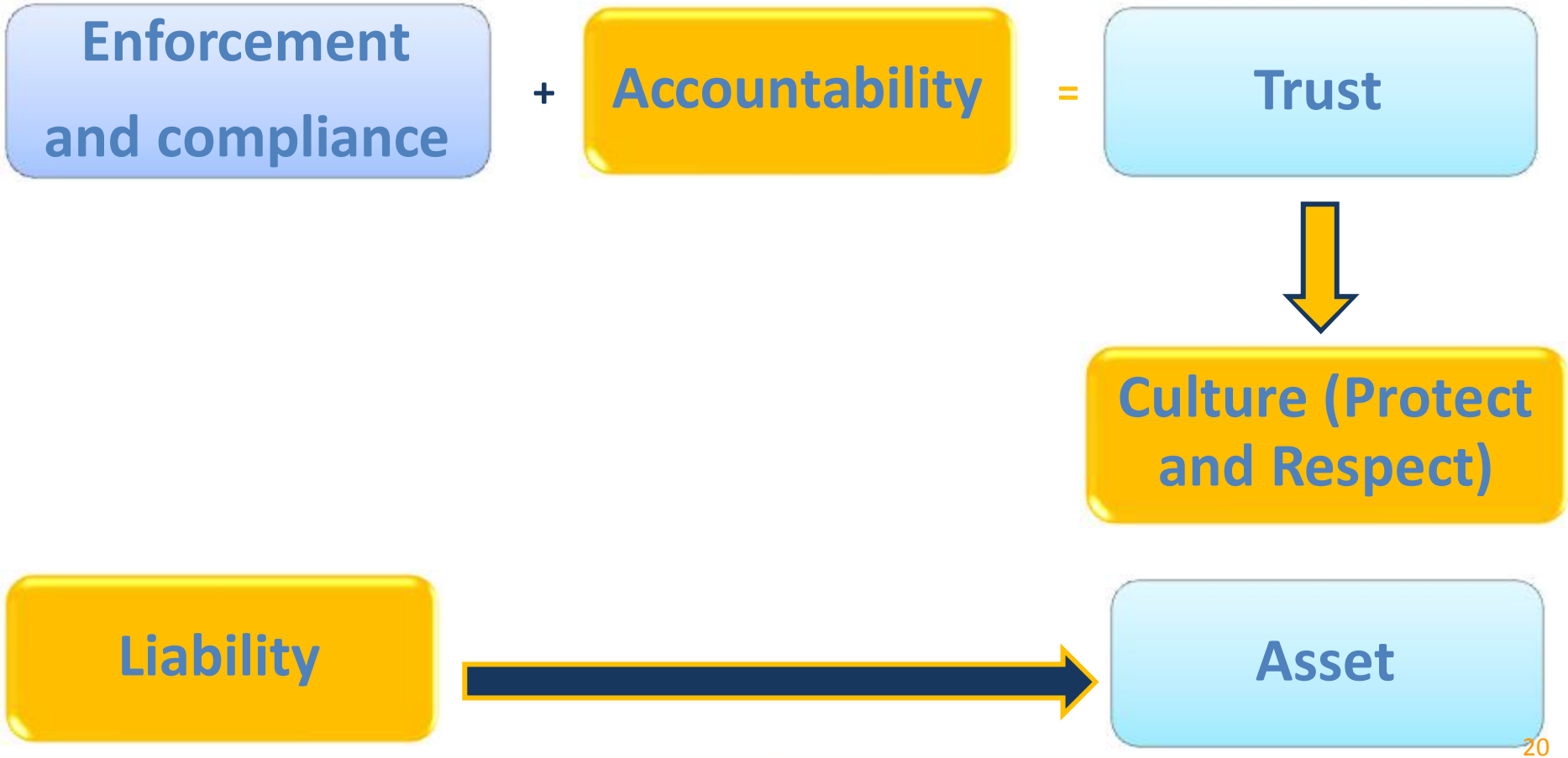
- Update personal data inventory
- Revise policies
- Treat risk assessment tools as evergreen
- Update training and education
- Adapt breach and incident response protocols
- Fine-tune data processor management

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

Effect of Paradigm Shift



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)

Tips for In-house Counsel


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

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

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

PCPD.org.hk