

**Effective Governance to deal with Cybersecurity, Emerging Technology
Risks, and Privacy.
ISACA Annual Conference**

Privacy Management Programme - A pathway to Privacy Governance

Stephen Kai-yi Wong

Privacy Commissioner for Personal Data, Hong Kong


17 March 2016



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

PCPD.org.hk

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



Nowadays, leaving a digital footprint is inevitable



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

PCPD.org.hk

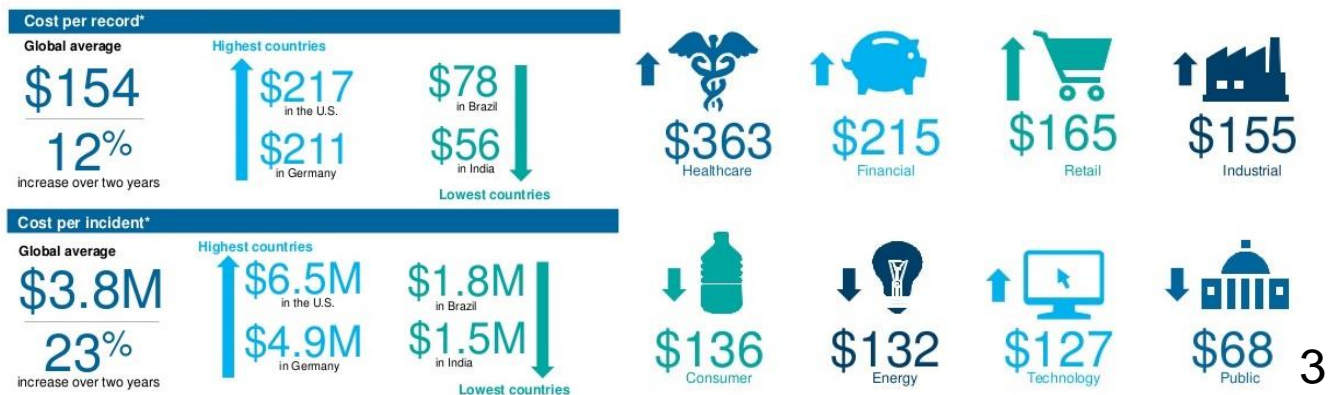
保障、尊重個人資料
Protect, Respect Personal Data

Responsibilities

Individuals – Mind your digital footprints



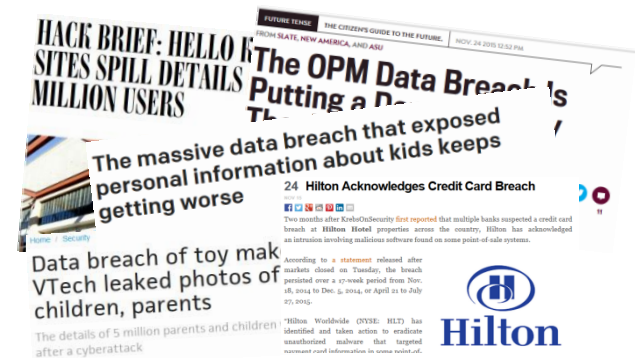
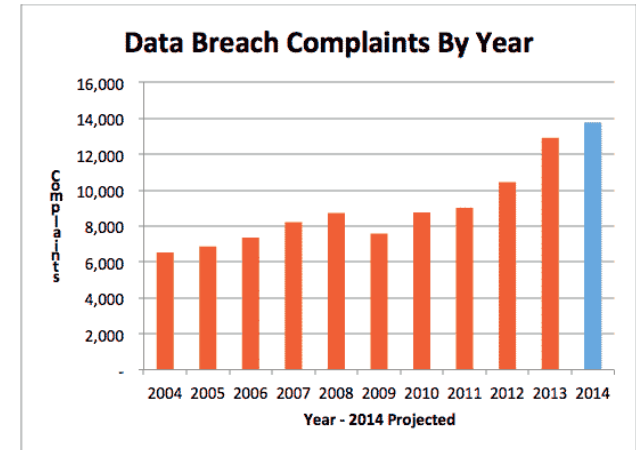
Corporates – Protect and respect personal data



Data Breach Trend on the Increase

“Data breach is no longer a question of IF, but a question of WHEN...”

Governance + control + best practice = Trust from customers



Paradigm Shift

Conventional wisdom of data protection:

- ✓ A Legal/compliance matter
- ✓ Not a top management concern

Paradigm shift is needed:

- ✓ **From Compliance**
to Accountability



Privacy Management Programme Pledging Organisations



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.



Privacy Management Programme Pledging Ceremony



7



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

PCPD.org.hk

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

Privacy Management Programme Best Practice Guide

Media Statements

Date: 18 February 2014

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

(18 February 2014) The Office of the Privacy Commissioner for Personal Data ("**PCPD**") released today Privacy Management Programme: A Best Practice Guide (the "Guide"). The Guide outlines the building blocks of Privacy Management Programmes ("**PMP**"), a strategic framework to protect personal data privacy. |

**Privacy
Management**
Programme
A Best Practice Guide

8



PMP Best Practice Guide Framework

- Three top-down management commitments;
- Seven bottom-up programme controls;
- Two on-going monitoring processes.

Privacy Management Programme – At A Glance

Part A Baseline Fundamentals

Organisational Commitment		
Buy-in from the Top	Data Protection Officer/Office	Reporting
<ul style="list-style-type: none"> Top management support is key to a successful privacy management programme and essential for privacy-respectful culture 	<ul style="list-style-type: none"> Role exists and is involved where appropriate in the organisation's decision-making process Role and responsibilities for monitoring compliance of the Personal Data (Privacy) Ordinance are clearly identified and communicated throughout the organisation Responsible for the development and implementation of the programme controls and their ongoing assessment and revision Policy and procedures are in place to incorporate personal data protection into every major function involving the use of personal data 	<ul style="list-style-type: none"> Reporting mechanisms need to be established, and they need to be reflected in the organisation's programme controls

Part B Ongoing Assessment and Revision

Oversight & Review Plan
<ul style="list-style-type: none"> Develop an oversight and review plan <p>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.</p>

Assess & Revise Programme Controls Where Necessary

<ul style="list-style-type: none"> 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 Improve communication
--

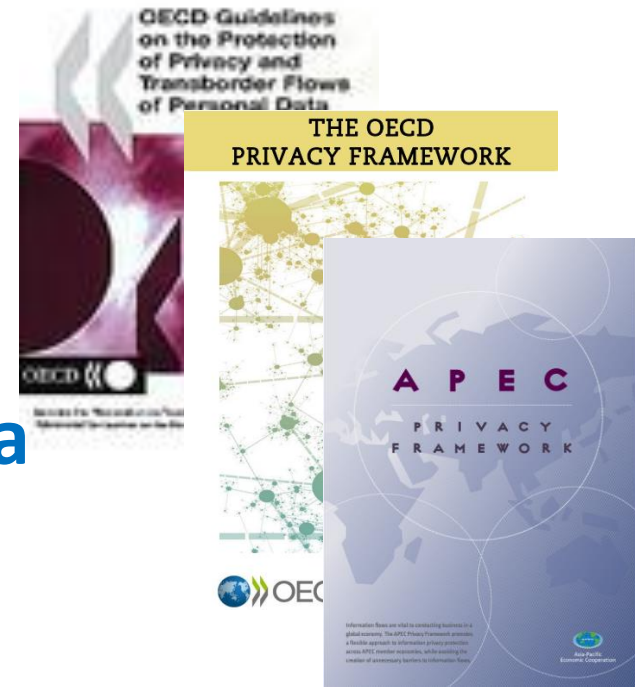
Programme Controls The following programme controls are in place:		
Personal Data Inventory	Policies	Risk Assessment Tools
<ul style="list-style-type: none"> The organisation is able to identify the personal data in its custody or control The organisation is able to identify the reasons for the collection, use and disclosure of the personal data 	Covering: <ul style="list-style-type: none"> Collection of personal data Accuracy and retention of personal data Use of personal data including the requirements of consent Security of personal data Transparency of organisations' personal data policies and practices Access to and correction of personal data 	Training & Education Requirements
		Breach Handling
		Data Processor Management
		Communication



International privacy frameworks

Privacy management programme (PMP):

- Not mandatory in Hong Kong
- Demonstrates accountability
- Enshrined in international data protection principles such as those in OECD and APEC



10



More Jurisdictions are Embedding Accountability

Canada – Protection and Electronic Documents Act (PIPEDA), 2000



Korea – Personal Information Protection Act (PIPA), 2011

The Philippine – Data Privacy Act, 2012

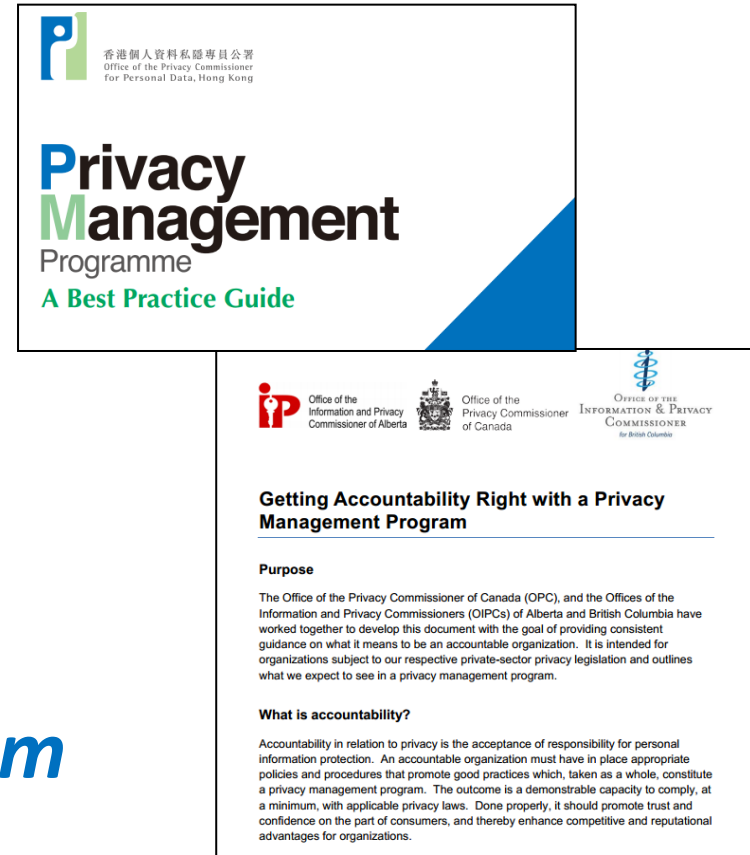
The EU – General Data Protection Regulation, effective in two years' time

Interoperability

The Hong Kong *Privacy Management Programme: A Best Practice Guide*

is modeled on the

Canada's *Getting Accountability Right with a Privacy Management Program*



Pilot Consultancy Service on Implementing PMP in the Public Sector

A consultancy service has been engaged to facilitate three HKSARG bureaux/departments to implement PMP

Deliverables (toolkits & training) will be beneficial to organisation implementing PMP



13



Privacy Mark – A Seal of Approval



Privacy Mark (P-Mark) Scheme:

- Recognition scheme for those implementing PMP beyond the requirement of the law;
- Allow consumers to differentiate organisations that respect personal data beyond the minimum requirement of the law;
- Recognition schemes are being considered worldwide such as the UK.

14



Respecting Customers' Personal Data

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



15



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

PCPD.org.hk

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

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

