McDonough School of Business
Georgetown University
Washington DC
7 April 2016

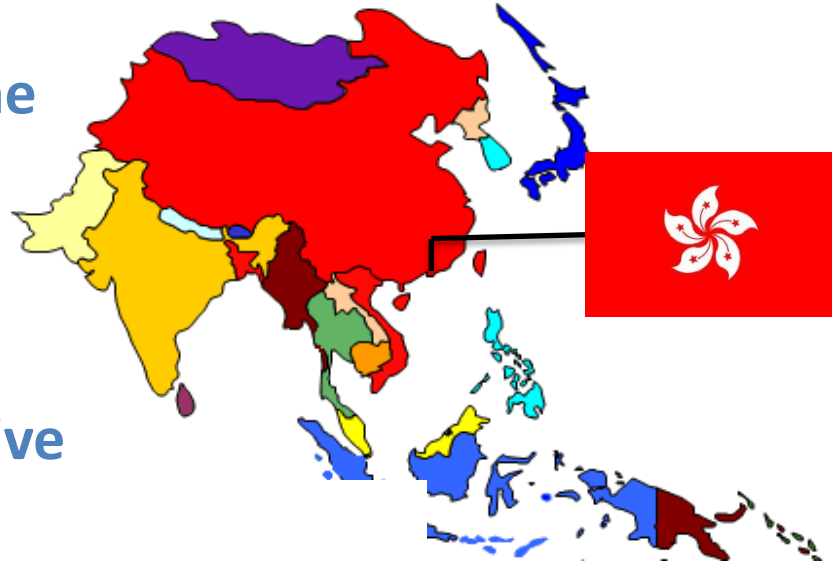
Hong Kong Personal Data Protection Regulatory Framework - An Approach to Consultative Regulation

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

The Hong Kong Data Protection Law

The Personal Data (Privacy) Ordinance 1995 (the Ordinance)

- comprehensive and stand-alone
  - 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



Definitions under the Ordinance

"Data subject"

- a living individual who is the subject of the "personal data" concerned

"Data user"

- a person who controls the collection, holding, processing or use of the personal data

Definitions under the Ordinance

"Personal data"

- relating directly or indirectly to a living individual
- from which it is practicable for the identity of the individual to be directly or indirectly ascertained
- in a form in which "access to" or "processing of" the data is practicable

Six Data Protection Principles (DPPs)

Principle 1 – Purpose and Manner of Collection

- related to the functions or activities of the data user
- lawful and fair means
- adequate but not excessive

Principle 1 – Purpose and Manner of Collection

Data subject be informed of:

- purposes of data collection
- classes of persons to whom the data may be transferred
- whether it is obligatory or voluntary for the data subject to supply the data
- where it is obligatory for the data subject to supply the data, the consequences for him if he fails to supply the data
- name or job title and address to which access and correction requests of personal data may be made

Principle 2 – Accuracy and Duration of Retention

Data users to take practicable steps to ensure:

- accuracy of personal data held by them
- personal data not being kept longer than is necessary for the purpose
- when engaging a data processor to process personal data, contractual or other means being adopted to prevent any personal data transferred to the data processor from being kept longer than necessary

Principle 3 – Use of Personal Data

- not being used for a new purpose without prescribed consent

"new purpose" - any purpose other than the purposes for which they were collected or directly related purposes

Principle 4 – Security of Personal Data

- practicable steps being taken to ensure no unauthorized or accidental access, processing, erasure, loss, use and transfer
- security in the storage, processing and transmission of data

Principle 5 – Openness – Information be Generally Available

Data users to provide

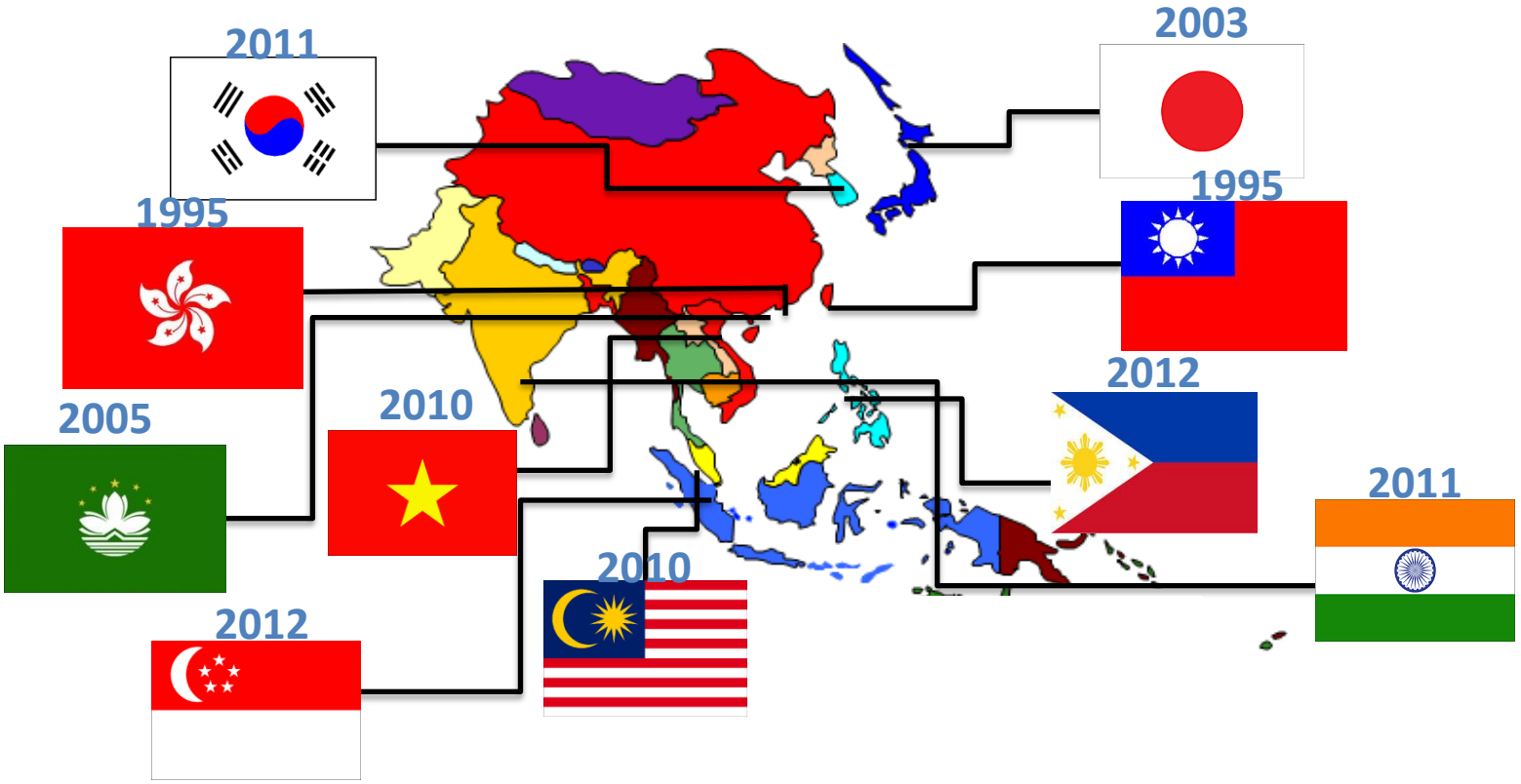
- policies and practices in relation to personal data
- kinds of personal data held
- main purposes for which personal data are used

Principle 6 – Access to Personal Data

Data subject be entitled to request

- access to his personal data
- correction of his personal data

The Personal Data Landscape in Asia



Relevant Consultation Activities of the PCPD (HK)

	2010	2011	2012	2013	2014	2015
Complaints received	1,179	1,486	1,213	1,792	1,702	1,971
Enquiries received	18,000	18,680	19,053	24,161	17,328	18,456

Regular opinion surveys on individuals and organisations :
1998, 1999, 2002, 2010, 2013, 2014, 2015

Relevant Consultation Activities of the PCPD (HK)

Specific consultations/surveys on topical issues:

- 2001/2002/2008/2011 Code of Practice for Consumer Credit Reference Agencies
- 2002 Employee Monitoring and Personal Data Privacy at Work
- 2006 Property Management Practice
- 2006 Hotel Management Practice
- 2006 Youth Attitude
- 2007 Use of the Internet by Youths
- 2008 Estate Agency Practice
- 2009/2010 Ordinance Review
- 2011 Property Management Practice
- 2012 Insurance Industry Practice
- 2013 Retail Industry Practice
- 2014 Banking Industry Practice
- 2015 Protection of Personal Data in Public Registers
- 2016 Electronic Health Record Sharing System

Industry-specific Privacy Campaign

- launched in January 2015
- theme = “Developing Mobile Apps: Privacy Matters”
- co-organised by 10 leading trade associations; supported by 10 ICT professional/academic institutions

Co-organisers:

Supporting Organisations:

Office of the Government Chief Information Officer

Industry-specific Privacy Campaign

- 13 activities with more than 2,400 participants
- will continue till April 2016

Data Protection Officers' Club

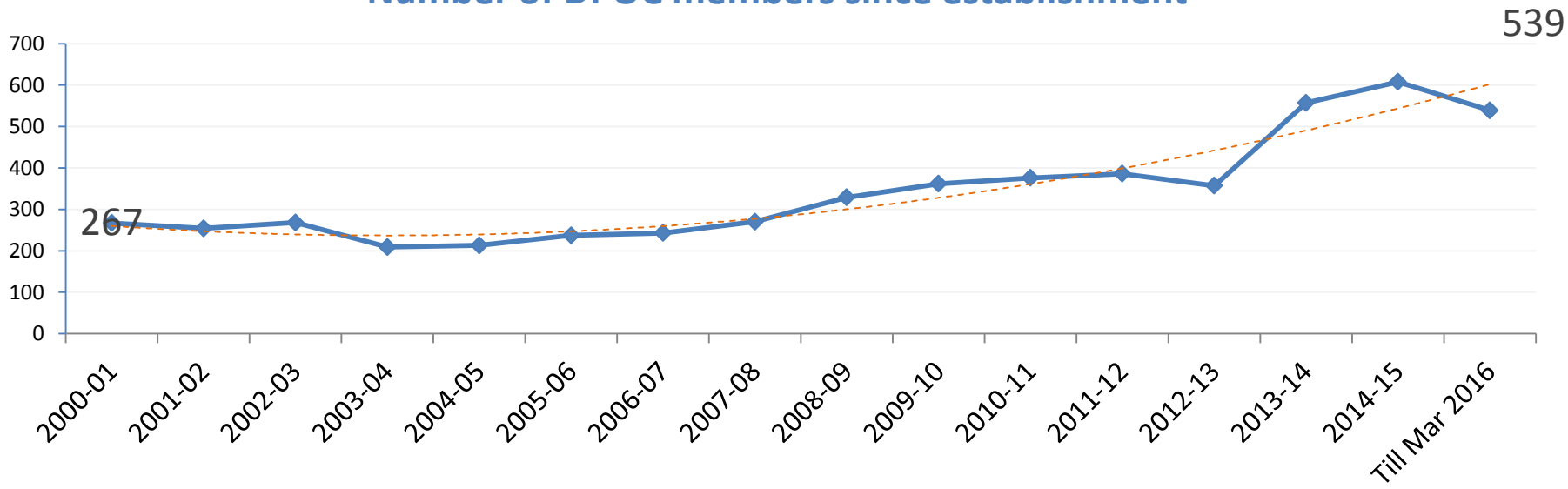
- provide practising data protection officers with a platform for
  - advancing their knowledge
  - experience sharing
  - training

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

Data Protection Officers' Club

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

Number of DPOC members since establishment



Meeting with Stakeholders

- the Commissioner and senior executives regularly meet with stakeholders of major trade associations, professional bodies and corporations in Hong Kong

Professional Compliance Workshops

- **77 workshops were held with over 2100 participants in 2015**

Workshop topics in 2016
• Data Protection and Data Access Request
• Data Protection in Banking/Financial Services
• Data Protection in Direct Marketing Activities
• Data Protection in Human Resource Management
• Data Protection in Insurance
• Data Protection in Retail Operation
• Legal Workshop on Data Protection
• Practical Workshop on Data Protection Law
• Privacy Management Programme

Support for Small-Medium Enterprises

- self-training module on protection of personal data for SMEs

Two Consultative Advisory Committees

Personal Data (Privacy) Advisory Committee:

- to advise the Commissioner on privacy matters

Two Consultative Advisory Committees

Standing Committee on Technological Developments:

- to advise the Commissioner on matters relevant to the developments in the processing of data and computer technology

Results of Consultation Activities

Code of Practice / Guidelines:

- Code of Practice on Consumer Credit Data
- Code of Practice on Human Resource Management
- Code of Practice on the Identity Card Number and Other Personal Identifiers
- Privacy Guidelines: Monitoring and Personal Data Privacy at Work

Results of Consultation Activities

Guidance Notes:

- Best Practice Guide for Mobile App Development
- Collection and Use of Personal Data through the Internet – Points to Note for Data Users Targeting at Children
- Guidance for Data Users on the Collection and Use of Personal Data through the Internet
- Guidance on CCTV Surveillance and Use of Drones
- Guidance on Collection and Use of Biometric Data
- Guidance on Data Breach Handling and the Giving of Breach Notifications
- Guidance on Electioneering Activities
- Guidance on Personal Data Erasure and Anonymisation
- Guidance on Personal Data Protection in Cross-border Data Transfer
- Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement
- Guidance on Property Management Practices
- Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry
- Guidance on the Proper Handling of Customers' Personal Data for the Insurance Industry
- Guidance on the Proper Handling of Data Correction Request by Data Users
- Guidance on the Use of Portable Storage Devices
- Guidance on Use of Personal Data Obtained from the Public Domain
- Human Resources Management
- New Guidance on Direct Marketing
- Personal Data Privacy : Guidance for Mobile Service Operators
- Privacy Management Programme: A Best Practice Guide
- Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users

Results of Consultation Activities

Information Leaflets:

- A Guide for Data Users - Compliance with Data Access and Correction Requests
- About the Office of the Privacy Commissioner for Personal Data, Hong Kong
- An Overview of the Major Provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012
- Care for Patients - Protect Their Personal Data
- Cloud Computing
- Matching Procedure : Some Common Questions
- Offence for disclosing personal data obtained without consent from the data user
- Online Behavioural Tracking
- Outsourcing the Processing of Personal Data to Data Processors
- Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals)
- Personal Data Privacy Protection: What Mobile Apps Developers and their Clients should know
- Privacy Impact Assessments
- Privacy Implications for Organisational Use of Social Networks
- Understanding the Code of Practice on Human Resource Management - Frequently Asked Questions About Recruitment Advertisements

Online Resources

- online training platform
- Code of Practices / Guidelines, Guidance Notes, Information Leaflets

Octopus Card

Stored-value payment card

- Payment for public transport underground/train/bus/ferry
- Corner shops, supermarkets, fast-food stores
- On and off street parking
- Access to residential and commercial building

"Octopus Incident" 2010

Octopus Rewards Limited ("Octopus")

"Octopus Rewards Programme"

Octopus card + personal data ⟶ Member

Member ⟶ purchase from Octopus's business partners (e.g. retail shops, restaurants and insurance companies)

- Earn Reward Dollars (Reward$1 = HK$1)
- Reward Dollars - redeem goods and services from Octopus business partners

Octopus shared members' personal data with six of its business partners for monetary gains without informing members of such sale.

“Octopus Incident” 2010

Personal Data collected for the management of Octopus Card

Sold

Insurance Companies for making Direct Marketing calls without informing their members of such sales

“Octopus Incident” 2010

South China Morning Post EDITION: HONG KONG

HONG KONG | NEWS | BUSINESS | TECH | LIFESTYLE | COMMENT | SPORT | PRO

Octopus sold personal data of customers for HK$44m

Phyllis Tsang and Ng Kang-chung

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life

ASIA TECHNOLOGY

Octopus CEO Resigns Over Data Sale

By JEFFREY NG

Updated Aug. 4, 2010 11:43 a.m. ET

CHINADAILY

Thursday, Mar 10, 2016 中国日报

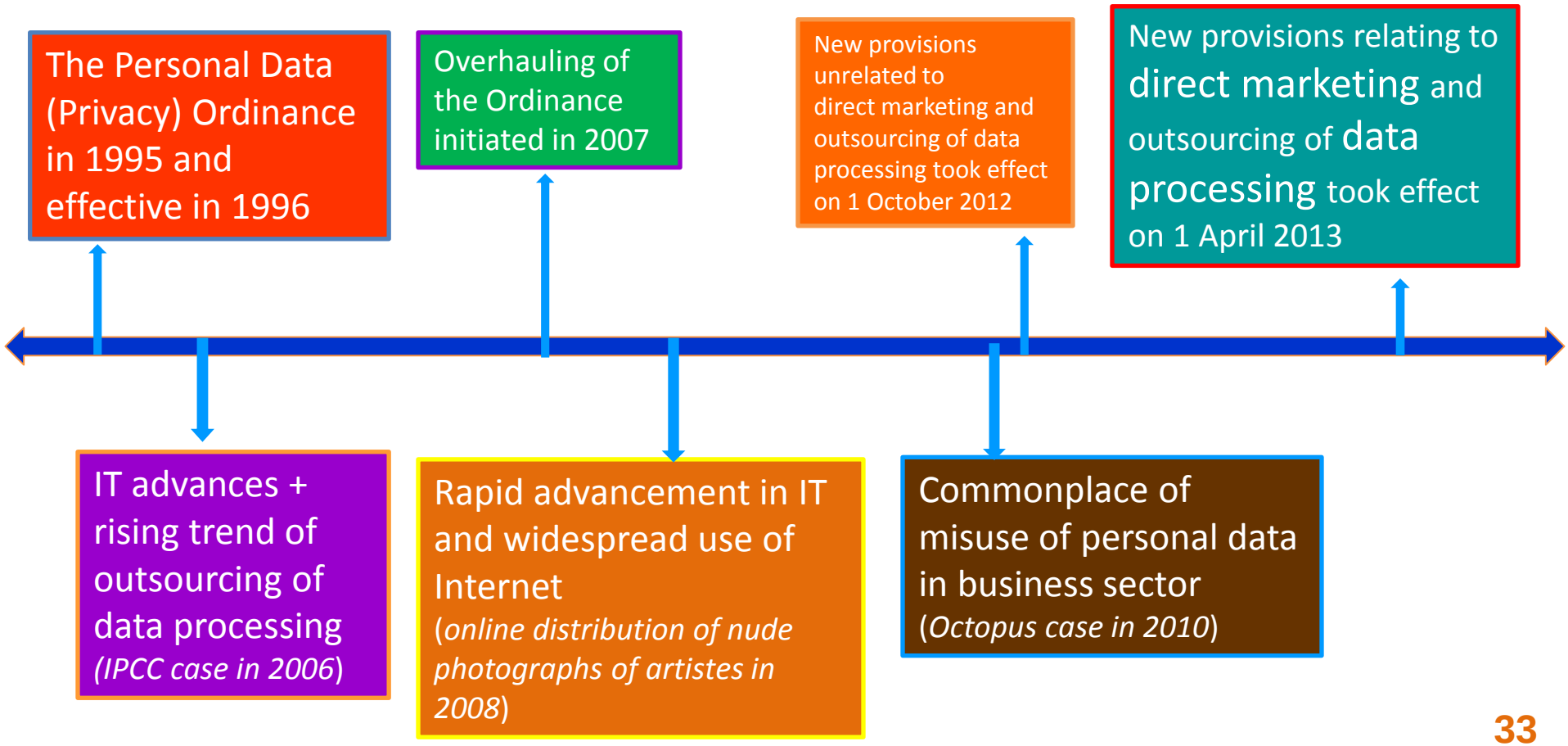
Home | China | Business | Metro Beijing | Regional | World | Opinion | Spor

Hong Kong

Octopus chairman to step down in Dec

By Michelle Fei (HK Edition)
Updated: 2010-10-20 06:57

Timeline & Background of the Amendment Ordinance, 2012



Amendments in 2012 upon Consultation

Direct marketing (s.35A-M)

Outsourcing of personal data processing (DPP2(3) and DPP4(2))

Criminalising the disclosure of personal data obtained without data user's consent (s.64)

Legal assistance to aggrieved individuals

Strengthening the Privacy Commissioner's enforcement power

New exemptions (self-incrimination, legal proceedings etc.)

New Provisions (Overview)

Direct Marketing	• Companies have been revising their regimes and adjusting their privacy policies and practices accordingly
Outsourcing of personal data processing	• Large businesses would generally use contractual means to bind the retention, secondary use, and security of personal data handled by data processors. However, this practice may not be prevalent among SMEs
Criminalising the disclosure of personal data without data user's consent	• Agents are prohibited from disclosing customers' personal data obtained from their principals for other purposes (Agency companies bear criminal liability)

New Provisions on Direct Marketing Activities

Prior to 1 April 2013 : "opt-out" mechanism (s.34)

After 1 April 2013 : "opt-in" mechanism, respect data subject's right of self-determination (new provision s.35A-M)

Catalyst cause : inappropriate handling of personal data by "Octopus" and various large-sized organisations such as banks, telecommunications and insurance companies for direct marketing purposes

Problems Revealed in Octopus Incident & the Remedies in New Direct Marketing Provisions

Problems revealed	New measures against data users
No requirement for "opt-in" at the collection stage (*Not even an opt-out option in the Octopus Incident*)	• Must take specified actions and obtain data subject's express consent before using personal data for direct marketing
Personal data was shared with business partners for **monetary gains** without obtaining data subject's prescribed consent	• Must take specified actions and obtain data subject's consent before such transfer to third party for direct marketing

Insignificant fine for breach of opt-out request (repealed) : maximum fine of HK$10,000	• Maximum penalty for breach:
	  • fine of HK$1,000,000 **and** 5 years' imprisonment (transfer personal data for direct marketing for gain);
	  • HK$500,000 and 3 years (for others)

New Provisions on Outsourcing of Personal Data Processing (DPPs 2 & 4)

Issues to be dealt with	New requirements
Data processor's unnecessary retention of personal data obtained from data user	If a data processor is engaged, whether within or outside HK, data user must adopt contractual or other means to prevent: - unnecessary retention by the data processor (DPP 2) - unauthorised or accidental access, loss or use of data transferred for processing purposes (DPP 4)
Commonplace of unauthorised or accidental access, processing, erasure, loss or use of personal data transferred to data processor	

Impact on Business

Public awareness (direct marketing and data processing):

- before
  - one seminar / month for 60 people
- after
  - demand on talks rocketed
  - average 8-10 seminars /month
  - targeting more specialised audience (finance, HR, IT, insurance, and direct marketing industries)

Impact on Business

Increased use of Privacy Impact Assessments (PIAs) by organisations:

- government – PIAs included in government projects that involve personal data (Transport Department - new speed camera, Immigration Department - smart ID card)

- private sector – sizable companies

Impact on Business

Criminalisation:

- the use of personal data by the data user, and the transfer of personal data to a third party by the data user, for direct marketing without the requisite notification to and consent from the data subject

Public's increased awareness:

- of their rights to personal data privacy resulting in more complaints to the business and to PCPD(HK)

Criminalising the Disclosure of Personal Data Obtained without Data User's Consent

Before the amendments

- **Breach of Collection Principle (DPP1) & Use Principle (DPP3)** → not criminal offence

After the amendments

- **Impact: Agents/individuals are prohibited from disclosing customers' personal data obtained from their principals for other purposes**
- The liabilities are on the offenders, and the business could only lighten their security against any such criminal acts committed by their employees and agents engaged by them.

Change of Business Attitude

A 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

Change of Business Attitude

Participating organisations have:

- **implemented activities that focus on legal compliance requirements and a specific Code of Practice (HR Management) issued by PCPD(HK)**
- **invested heavily in privacy and data protection measures related to technical and security measures, records retention, data privacy notices and policies, requirements for processors, and managing and responding to access requests**

Change of Business Attitude

- further developing the privacy management programme in training and awareness; managing third-party risk; access requests, inquiries and complaints; expanding privacy impact assessments programmes and implementing privacy by design procedures; and testing incident and breach protocols

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

Cross-border/boundary Data Transfer Requirements

Section 33 of the Ordinance (not yet in force): Data user shall not transfer personal data to a place outside Hong Kong unless:

a) the place is specified by the Commissioner as substantially similar/serving same purpose, as the Hong Kong data protection law

b) data user has reasonably grounds for believing that law exists in the place that is substantially similar/serving same purpose

c) consent from data subject has been obtained in writing

d) data user has reasonably grounds for believing that, among other things, the transfer is for the avoidance or mitigation of adverse action against the data subject

e) exempted in other parts of the Ordinance

f) data user has exercised all due diligence to ensure similar protection is afforded

Cross-border/boundary Data Transfer Requirements

In preparation for cross-border/boundary data transfer:

a) **PCPD(HK) has prepared a 'white-list' of jurisdictions with data protection laws substantially similar or serving same purpose**

b) **PCPD(HK) released a Guidance on Personal Data Protection in Cross-border Data Transfer to advise data users how they should prepare for the implementation**

c) **HK Government engaged a consultant to engage the business in conducting a business impact assessment**

Media Statements

Date: 29 December 2014

PCPD Publishes Guidance on Personal Data Protection in Cross-border Data Transfer

(29 December 2014) The Office of the Privacy Commissioner for Personal Data ("PCPD") published today a Guidance on Personal Data Protection in Cross-border Data Transfer (the "Guidance").

Section 33 of the Personal Data (Privacy) Ordinance (the "Ordinance") provides stringent and comprehensive regulation of transfer of data to outside Hong Kong. It expressly prohibits the transfer of personal data to places outside Hong Kong except in circumstances specified in the Ordinance. This ensures that the standard of protection afforded by the Ordinance to the data under transfer will not be reduced as a result of the transfer. However, section 33 of the Ordinance is not yet in operation.

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

Guidance Note

Guidance on Personal Data Protection in Cross-border Data Transfer

PART 1: INTRODUCTION

Section 33 of the Personal Data (Privacy) Ordinance (the "**Ordinance**") prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. The purpose of such cross-border transfer restriction is to ensure that the transferred personal data will be afforded a level of protection comparable to that under the Ordinance.

(a) The place is specified by the Privacy Commissioner for Personal Data (the "**Commissioner**") by notice in the Gazette that there is in force any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(b) The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance;

Privacy Management Programme (PMP)

"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."

privacy management programme → accountability

Privacy Management Programme (PMP)

- 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

Privacy Management Programme (PMP)

- from Compliance to Accountability:
  - Hong Kong Government
  - 25 insurance companies
  - 9 telecommunications companies
  - 5 organisations from other sectors
- all pledged to implement PMP

Privacy Management Programme

PMP Best Practice Guide

Three top-down management commitments:

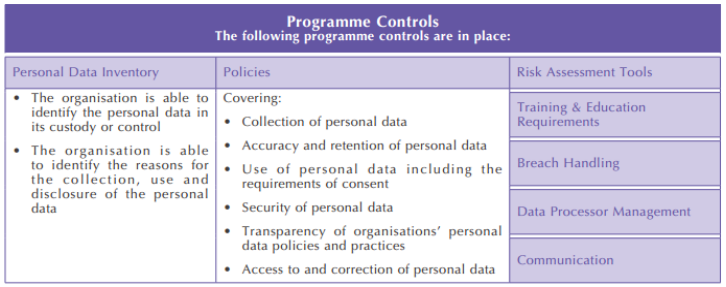
1. top-management commitment and buy-in
2. setting up of a dedicated data protection office or officer
3. establishing reporting and oversight mechanism for the privacy management programme

Organisational Commitment		
Buy-in from the Top	Data Protection Officer/Office	Reporting
• Top management support is key to a successful **privacy management programme** and essential for privacy-respectful culture	• 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	• Reporting mechanisms need to be established, and they need to be reflected in the organisation's programme controls

PMP Best Practice Guide

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
4. developing and maintaining training plan for all relevant staff
5. establishing workable breach handling and notification procedures
6. establishing and monitoring data processor engagement mechanism
7. establishing communication so that policies and practice are made known to all stakeholders

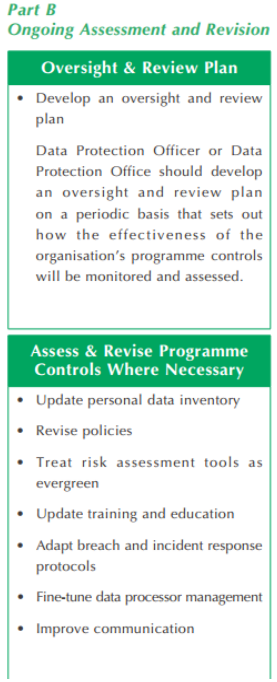


Programme Controls The following programme controls are in place:		
Personal Data Inventory	Policies	Risk Assessment Tools
• The organisation is able to identify the personal data in its custody or control • The organisation is able to identify the reasons for the collection, use and disclosure of the personal data	Covering: • 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

PMP Best Practice Guide

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.



Consultation 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

Privacy Mark – A Seal of Approval

Privacy Mark (P-Mark) Scheme:

- recognition scheme for those implementing privacy management programme beyond the requirement of the law
- customer-facing allowing consumers to differentiate organisations that are more privacy-friendly
- transparent assessment criteria and benchmarks
- annual re-assessment
- to be launched in July 2016

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

From Compliance to Accountability

Effect of Paradigm Shift

Enforcement and compliance + Accountability = Trust

Culture (Protect and Respect)

Liability  Asset

Hong Kong Personal Data Protection Regulatory Framework - An Approach to Consultative Regulation