Seminar for the Insurance Authority

17 January 2018; IA Office, Wong Chuk Hang

Personal Data Protection and Data Governance

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

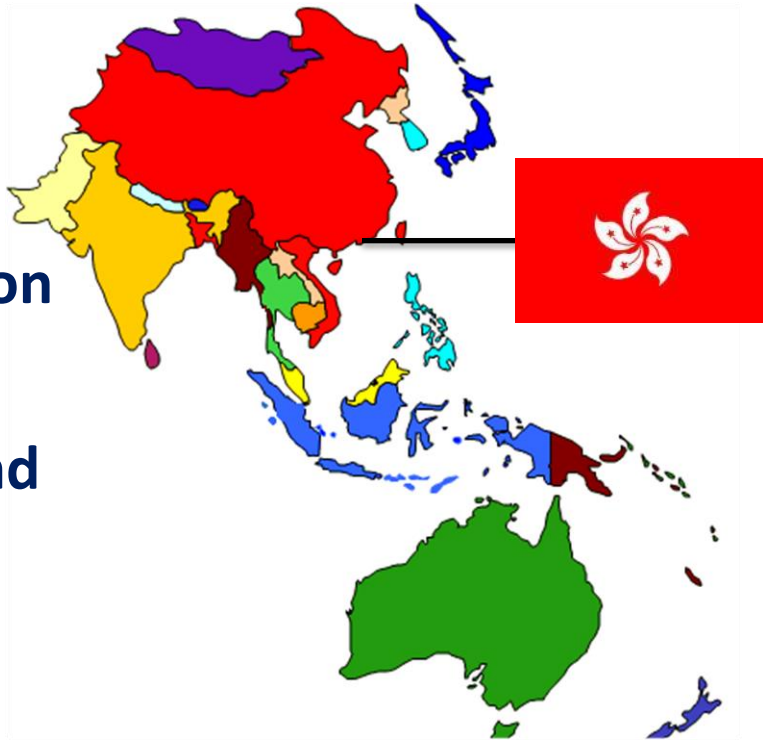
Presentation Outline

1. Introduction on PDPO and PCPD
2. Statistics and Case Sharing
3. Regulatory Strategies and Approach of PCPD
4. Privacy Implications of Cloud and Big Data
5. Privacy Management Programme (PMP)
6. Insurance Claims Database
7. Engagement with Stakeholders and the Public

1 Introduction on PCPD and PDPO

Personal Data (Privacy) Ordinance, Cap 486, Laws of Hong Kong

- Enacted in 1995
- Created independent Privacy Commissioner for Personal Data
- First comprehensive data protection law in Asia
- Covers the public (government) and private sectors
- Referenced to 1980 OECD Privacy Guidelines and 1995 EC Data Protection Directive



Legislative Intent

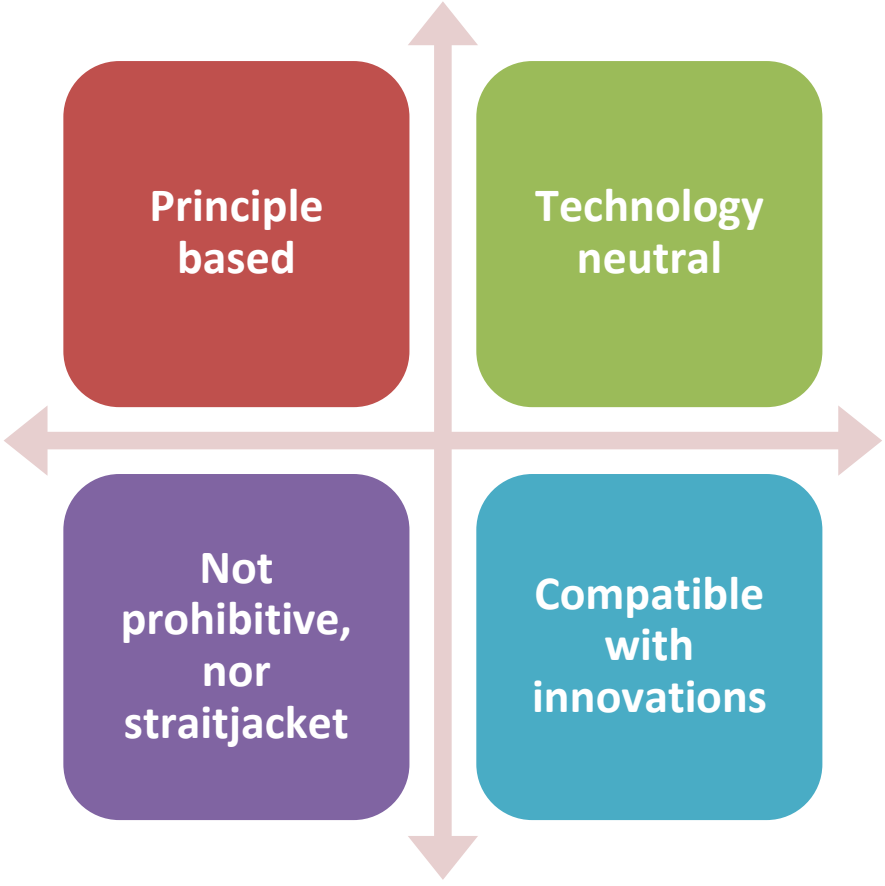
Business Perspective

- To facilitate business environment, maintain Hong Kong as a financial and trading hub

Human Rights Perspective

- Protect individuals' personal data privacy

Characteristics of the Ordinance



Role of the PCPD

An independent regulatory body

Headed by the Privacy Commissioner who is appointed by the Chief Executive of the HKSAR

Performs the functions and exercises the power conferred by the Personal Data (Privacy) Ordinance, e.g. :

- monitor and supervise compliance
- promote awareness and understanding
- examine proposed legislation
- undertake privacy-related research
- liaise and co-operate with counterparts outside Hong Kong

Key Provisions of the Ordinance

1. Definition of "Personal Data"?

"**Personal data**" (個人資料) means any **data** -

*(a) **relating** directly or indirectly to a living individual;*

*(b) from which it is practicable for the **identity** of the individual to be directly or indirectly ascertained; and*

*(c) in a **form** in which access to or processing of the data is practicable.*

"**Data**" (資料) means *any representation of information (including an expression of opinion) **in any document***.

2. Six Data Protection Principles of the Ordinance

1 收集目的及方式 Collection Purpose & 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移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

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 & Retention

資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的的實際所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept 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、處理、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

資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

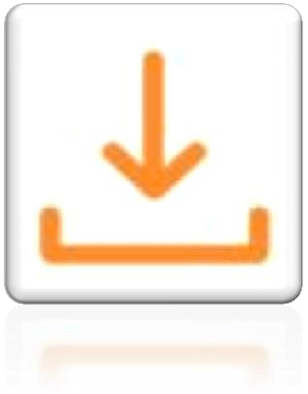
6 查閱及更正 Data Access & Correction

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.

Principle 1 – Purpose & Manner of Collection

- **Data collected must be-**
  - **related to the data user's functions or activities**
  - **adequate but not excessive**



- **The means of collection must be lawful and fair**
- **Must notify data subjects of collection purposes and the classes of persons to whom the data will be transferred, etc.**

Principle 2 – Accuracy & duration of retention

- **Data users shall take all practicable steps to ensure:**
  - **the accuracy of personal data held by them, and**
  - **the destruction of personal data after the purpose of use is satisfied**

Principle 3 – Use of personal data

- **Personal data shall not, without the prescribed consent of the data subject, be used for a *new purpose***

"Prescribed consent" means express consent given voluntarily which has not been withdrawn in writing

"New purpose" means any purpose other than (i) the purposes for which the personal data were collected and (ii) other directly related purposes

Principle 4 – Security of personal data

- Data users shall take **all practicable steps** to **safeguard** personal data against unauthorised or accidental access, processing, erasure, loss or use

Principle 4 – Security of personal data

- **What is "all practicable steps"?**

  - No statutory definition
  - No hard and fast rule for determination
  - A totality of facts approach
  - With considerations as to: (non exhaustive)

    - size, nature and resources of the data user
    - complexity of the data user's operations and its business model
    - amount and sensitivity of personal data held
    - likelihood of adverse consequences for affected individuals

Principle 4 – Security of personal data

- **Possible security measures** (non-exhaustive)

  - Organisational measures
    - Clear security policy and procedures
    - Privacy and security risk assessment
    - Regular and sufficient staff training
    - Audit log for system activities

  - Technical measures
    - Use, and regular update and patch of security software
    - Encryption of data
    - Restricted access to systems (on need basis)
    - Intrusion prevention and detection measures

Principle 4 – Security of personal data

- **Case sharing – A HK toy-maker**

  - Customer database hacked in late 2015
  - Data of about 6 million parents and 6.6. million children leaked
  - Investigation findings (among other things):
    - lack of testing and maintenance to identify and mitigate vulnerabilities
    - inadequate administrative access controls
    - various cryptographic deficiencies
    - absence of security monitoring and logging to detect potential threats
    - no overarching comprehensive security management program

Principle 5 – Information to be generally available (Transparency)

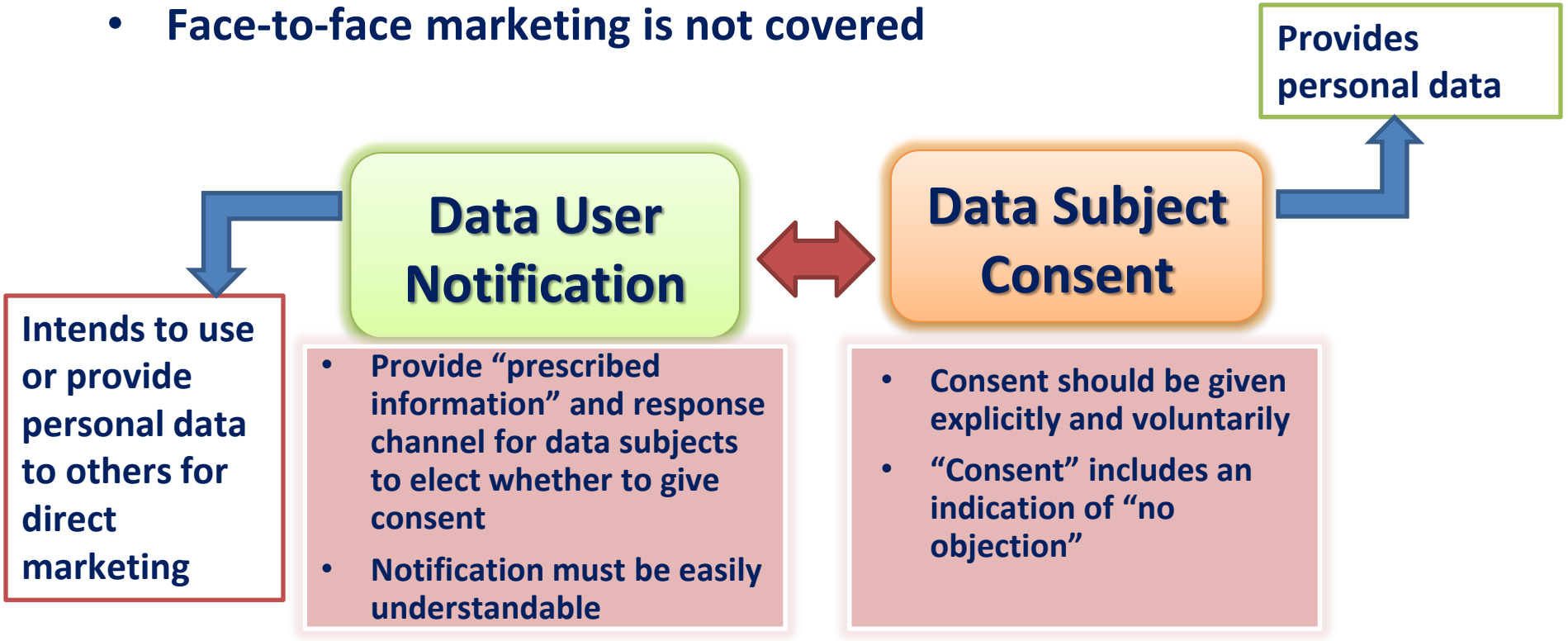
- Data users shall **provide or disclose**:
  - **policies and practices** in relation to handling of personal data
  - the **kinds of personal data** held
  - the **main purposes** for which personal data are used

Principle 6 – Access to personal data

- Data subject is entitled to request access to and correction of his personal data
- Data user may charge a non-excessive fee
- Data user shall respond within 40 days

3. Direct Marketing Requirements

- **Direct marketing activities** under the Ordinance include such activities made to **specific persons** by mail, fax, email and phone
- Face-to-face marketing is not covered



Direct Marketing Requirements

- Data user must comply with the data subject's **opt-out request** without charge [section 35G]

- **Criminal sanctions** apply if data user fails to comply with requirements of notification, consent and opt-out requests

Convicted Cases Relating to Direct Marketing

Date: April 2016

An insurance agent used personal data in direct marketing without taking specified actions and obtaining the data subject's consent, contrary to section **35C** of the Ordinance.

The agent also failed to inform the data subject of his opt-out right when using his personal data in direct marketing for the first time, , contrary to section **35F** of the Ordinance.

Penalty: Community Service Order of 80 hours for each charge

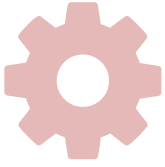
4. Cross-border Data Transfer

Section 33 of the PDPO prohibits transfer of personal data outside Hong Kong unless under 6 specified circumstances

Legislative intent: To ensure personal data transferred outside Hong Kong is afforded with same protection

Meaning of Transfer

Section 33 covers 2 situations:



Transfer from Hong Kong to a place outside Hong Kong

Transfer between 2 other places where the transfer is controlled by a data user in Hong Kong

Exceptions: s.33(2)(a) – (e)

Data user shall not transfer personal data outside Hong Kong unless one of the conditions are met:-

s.33(2)(a)	• Fall within one of the White List jurisdictions (i.e. the law in that place is *"substantially similar to or serves the same purposes as"* the PDPO pursuant to PCPD's assessment) [Note: The White List is to be kept confidential currently]
s.33(2)(b)	• Data user's own assessment (that the law in that place is *"substantially similar to or serves the same purposes as"* the PDPO)
s.33(2)(c)	• Data subject's written consent to the transfer
s.33(2)(d)	• Avoidance or mitigation of adverse action against the data subject
s.33(2)(e)	• Exemptions from data protection principle 3 (i.e. use limitation) under Part VIII of the PDPO apply

Exceptions: s.33(2)(f)

s.33(2)(f)

- **Data user has taken all reasonable precautions and exercised all due diligence such that personal data transferred will not be handled in a manner that contravenes the PDPO ("Due Diligence Requirement")**

Through either:

Contractual means; or

Non-contractual means

Exceptions: s.33(2)(f) – Contractual means

An enforceable contract between the parties to the transfer to ensure that the personal data is given equivalent protection

Recommended Model Clauses ("RMC")

- **A set of RMC set out in PCPD's guidance[1] to assist data users to develop an enforceable contract to satisfy the Due Diligence Requirement**
- **Does not require strict adoption by parties in cross-border transfer (greater flexibility)**
- **Can be a separate data transfer agreement or incorporated into a wider outsourcing agreement**

[1] Guidance on Personal Data Protection in Cross-border Data Transfer (December 2014): https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_crossborder_e.pdf

Exceptions: s.33(2)(f) – Contractual means

Terms can be modified or adapted to suit business needs

- Section I - Core Clauses
- Section II – Additional Clauses

Deals with:-

- transferor's obligation
- DPPs to be observed by transferee;
- parties' rights in the event of breach;
- audit requirement;
- sub-transfer;
- liabilities; and
- termination

Exceptions: s.33(2)(f) – Non-contractual means

Transferor may adopt the following measures (non-exhaustive):

<u>Transferor</u> has the right to conduct regular audit and inspection

<u>Transferor</u> to ensure the transferee has:

- sufficient technical competence and organisational measures on data protection with good track record
- robust data protection policies and procedures (e.g. data not kept longer than is necessary, data subjects' rights to access and correct their personal data, adequate staff training, etc.)
- (for intra-group transfer) internal safeguards and policies to reflect the requirements of the PDPO

Tips for Cross Border Data Transfer

Review existing data transfer strategy

Control unintended or unnecessary cross-border data transfer

Check the White List (when it comes into effect)

May adopt multiple measures to give more protection (e.g. even if the jurisdiction falls within the White List, the parties may still enter into a data transfer agreement)

Keep inventory of personal data (monitor transferee' data handling policies/ whereabouts of personal data)

Be transparent about cross border transfer

5. Exemptions
(Part 8 of PDPO)

Note:

(1) **No specific exemption** for government or public bodies (except personal data held by Government for safeguarding security, etc. in respect of Hong Kong – s.57);

(2) Exemptions under Part 8 of PDPO applicable to all data users

1. Request for access to information by data subjects under DPP6 and Part 5 of PDPO

Relevant Process – s.55(1)

- DPP6 and s.18(1)(b) is exempted (i.e. no need to comply with a data access request) until completion of a relevant process in determining suitability, eligibility or qualification of the data subject for employment or appointment to office, etc.
- Only applies to process where an appeal may be made against the determination

1. Request for access to information by data subjects under DPP6 and Part 5 of PDPO

Crime, etc. – s.58(1)

➢ **DPP6 and s.18(1)(b) is exempted if compliance with a data access request would be likely to:**

- **prejudice any purpose under s.58(1); or**
- **identify the person who is the source of the data**

1. Request for access to information by data subjects under DPP6 and Part 5 of PDPO

➢ **Examples of purposes under s.58(1) that may be applicable to IA:**

- **Prevention or detection of crime – s.58(1)(a);**
- **Prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice – s.58(1)(d);**

1. Request for access to information by data subjects under DPP6 and Part 5 of PDPO

➢ **Examples of purposes under s.58(1) that may be applicable to IA (cont'd):**

- **Prevention or preclusion of significant financial loss arising from imprudent business practices or malpractice – s.58(1)(e)**
- **Ascertaining whether the character of the data subject is likely to have significant adverse impact on the discharge of statutory functions – s.58(1)(f)**
- **Discharging statutory functions of a financial regulator – s.58(1)(g)**

1. Request for access to information by data subjects under DPP6 and Part 5 of PDPO

Legal professional privilege – s.60

- **DPP6 and s.18(1)(b) is exempted if the data consists of legal professional privileged information**

2. Request for access to information by law enforcement authorities

Crime, etc. – s.58(2)

- **DPP3 (Data Use Principle) exempted if:**
  - ➢ **data is used for any purpose under s.58(1); and**
  - ➢ **prejudice test is satisfied:**
    - **application of DPP3 would be likely to prejudice the purpose**
    - **data user to show reasonable grounds of its belief**

2. Request for access to information by law enforcement authorities

- **Reasonable enquiries made to law enforcement authorities before invoking exemption to release information:**

  (1) purpose for which the data is to be used;
  (2) reason why the data is relevant to or necessary for the purpose;
  (3) reason why data subject's consent is not obtained;
  (4) whether the data can be obtained from other source; and
  (5) in particular, how the application of DPP3 would be likely to prejudice the purpose.

3. Request for access to information by foreign government or regulators

Crime, etc. – s.58(2)

- **Exemption applies if the crime concerned is:**
  - ➢ **An offence under the laws of Hong Kong;**
  - ➢ **An offence under the laws of a place outside Hong Kong, if personal data is held or used in connection with legal or law enforcement cooperation between Hong Kong and that place - s.58(6)**

3. Request for access to information by foreign government or regulators

Disclosure authorised by law – s.60B(a)

- DPP3 (Data Use Principle) is exempted if use of data is required or authorised by law or court order in Hong Kong
  - ➢ IA may disclose information to an overseas regulator performing similar functions of IA under s.53B, Insurance Ordinance (Cap 41)

Legal proceedings, etc. – s.60B(b) & (c)

- DPP3 is exempted if use of data is:
  - ➢ Required in connection with legal proceedings in Hong Kong – s.60B(b)
  - ➢ Required for establishing, exercising or defending legal rights in Hong Kong – s.60B(c)

  e.g. taking legal advice for the purpose of defending his legal rights in future potential dispute – ***AAB No. 55 of 2015***

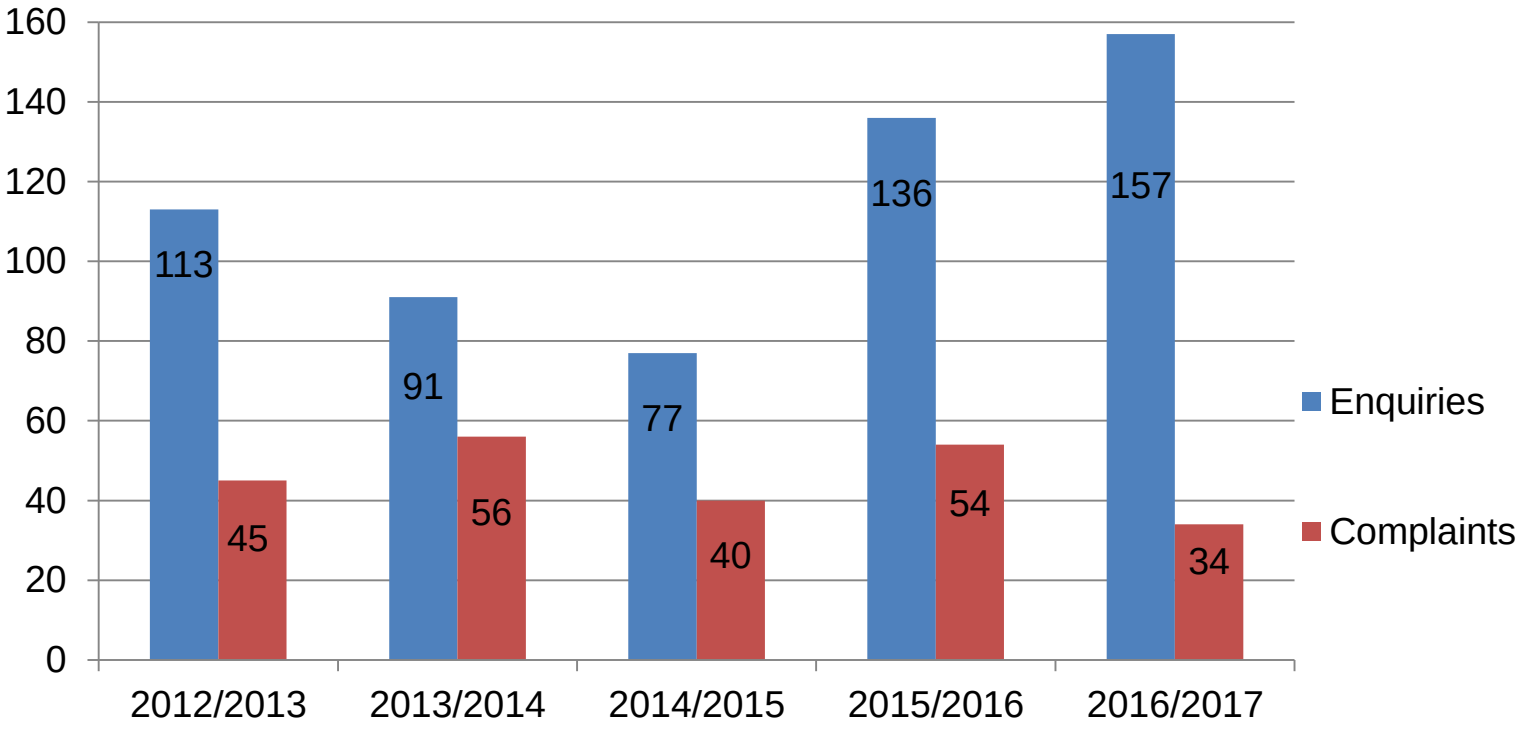
Secrecy obligation vs Data Access Request

- **Refusal to comply with a data access request by reason of s.20(1) (i.e. compliance is prohibited under any other ordinance)**

- **Information concerning an investigation carried out by IA (s.53A, Insurance Ordinance imposes secrecy obligation)**
  - ➢ **Must examine the requested information**
    - **e.g. AAB concluded that the information requested for (e.g. transaction details) originated from the bank itself and was not something it came to know or possess or obtain in the course of investigation by the HKMA – *AAB No. 10 of 2013* *(Note: the bank tried to rely on the secrecy obligation under s.120 of the Banking Ordinance)***

2 Statistics and Cases Sharing

Number of Enquiries and Complaints Relating to Insurance Industry



Number of Enquiries and Complaints Relating to Insurance Industry

Enquiries and complaints mainly concern:

DPP 1(1)	- Excessive collection of subscribers' personal data during insurance applications and in the course of handling insurance claims
DPP 3	- Disclosure of policyholders' personal data to third parties (e.g. relatives) without consent
DPP 4	- Loss of personal data (e.g. insurance application forms) - Personal data accessed by unauthorised parties
Direct Marketing	- Failure to take specified action before DM - DM without consent
DPP 6	- Failure to comply with data access request (e.g. medical reports)

Case sharing (1) – Adding Customer's Name and Mobile Number into WhatsApp Group

A MPF intermediary added a customer to his WhatsApp group for circulating MPF related information

Thereby disclosed the customer's name and mobile number to members of the group

No consent from the customer

Contravention of DPP3

Case sharing (2) – Use of Customers' Data for Internal Training

Regional Director of an insurer used insurance policy information of a former agent in a training, and disclosed the agent's name and other personal data, as well as the malpractice undertaken by the agent

Insurer argued that it was necessary to identity the parties concerned being someone the trainees knew so as to raise vigilance and deterrence to malpractice

The Regional Director's act was out of the agent's reasonable expectation to use his personal data

Not necessary to disclose the agent's identity to raise awareness; mere mentioning of capacity or roles of the agent involved would suffice

Contravention of DPP3 by insurer (vicarious liability through the Regional Director)

Case sharing (3) – Leakage of Customers' Data on the Internet

Database of 600 customers of an insurer leaked on the internet
(personal data involved: names, dates of birth, addresses, telephone numbers and details of policies)

↓

Caused by inappropriate granting of access right to the insurer's database

↓

The insurer failed to take sufficient measures to safeguard the personal data of its customers and hence contravened the requirements of DPP4

3 Regulatory Strategies and Approach of PCPD

Meeting Changing Needs

- Keep abreast of technological development
- Monitor international development and trend
- Keep track of evolving local privacy expectation

Corporate Governance

- Adhere to the principles of transparency and accountability
- Maximise utilisation of resources to achieve economy, efficiency and effectiveness
- Make continuous effort to streamline work procedures
- Apply a "selective in order to be effective" approach in priortising work, with an emphasis on assignments that will have the greatest impact
- Build and maintain a loyal and professional team

Promotion

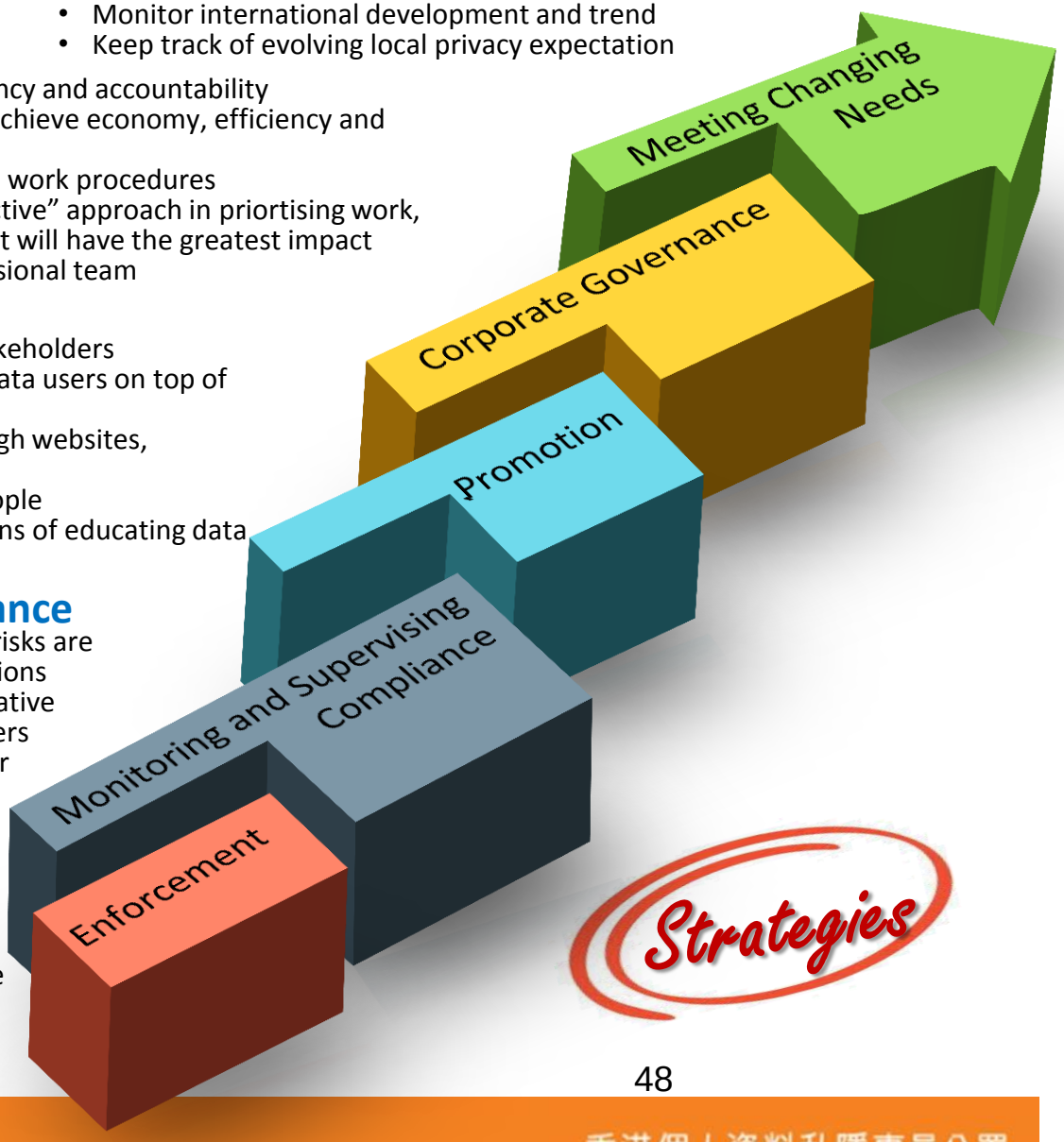
- Proactively seek the holistic engagement of stakeholders
- Promote best practices among organisational data users on top of meeting minimum legal requirements
- Maximise publicity and education impact through websites, publications and media exposure
- Engage the community, in particular, young people
- Use lessons learnt from investigations as a means of educating data users and data subjects

Monitoring and Supervising Compliance

- Check and investigate into areas where the privacy risks are significant and upon receipt of data breach notifications
- Partner with other regulators, leveraging their legislative mandates, institutional tools and enforcement powers
- Partner with overseas data protection authorities for handling cross-border privacy issues

Enforcement

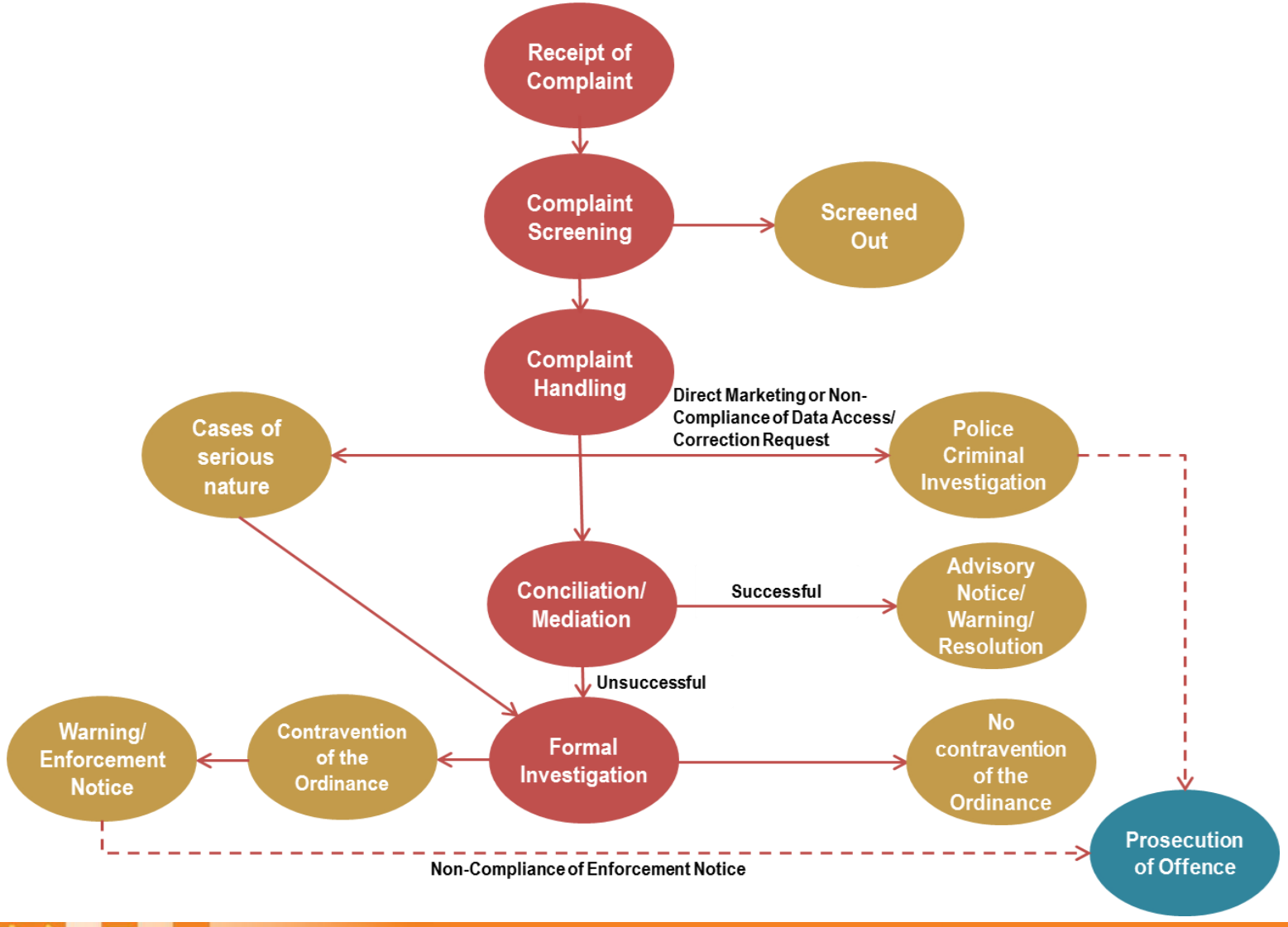
- Ensure equity, fairness and operational efficiency
- Act independently, impartially and without fear or favour
- Partner with other regulators, leveraging their legislative mandates, institutional tools and enforcement powers
- Partner with overseas data protection authorities for handling cross-border privacy issues



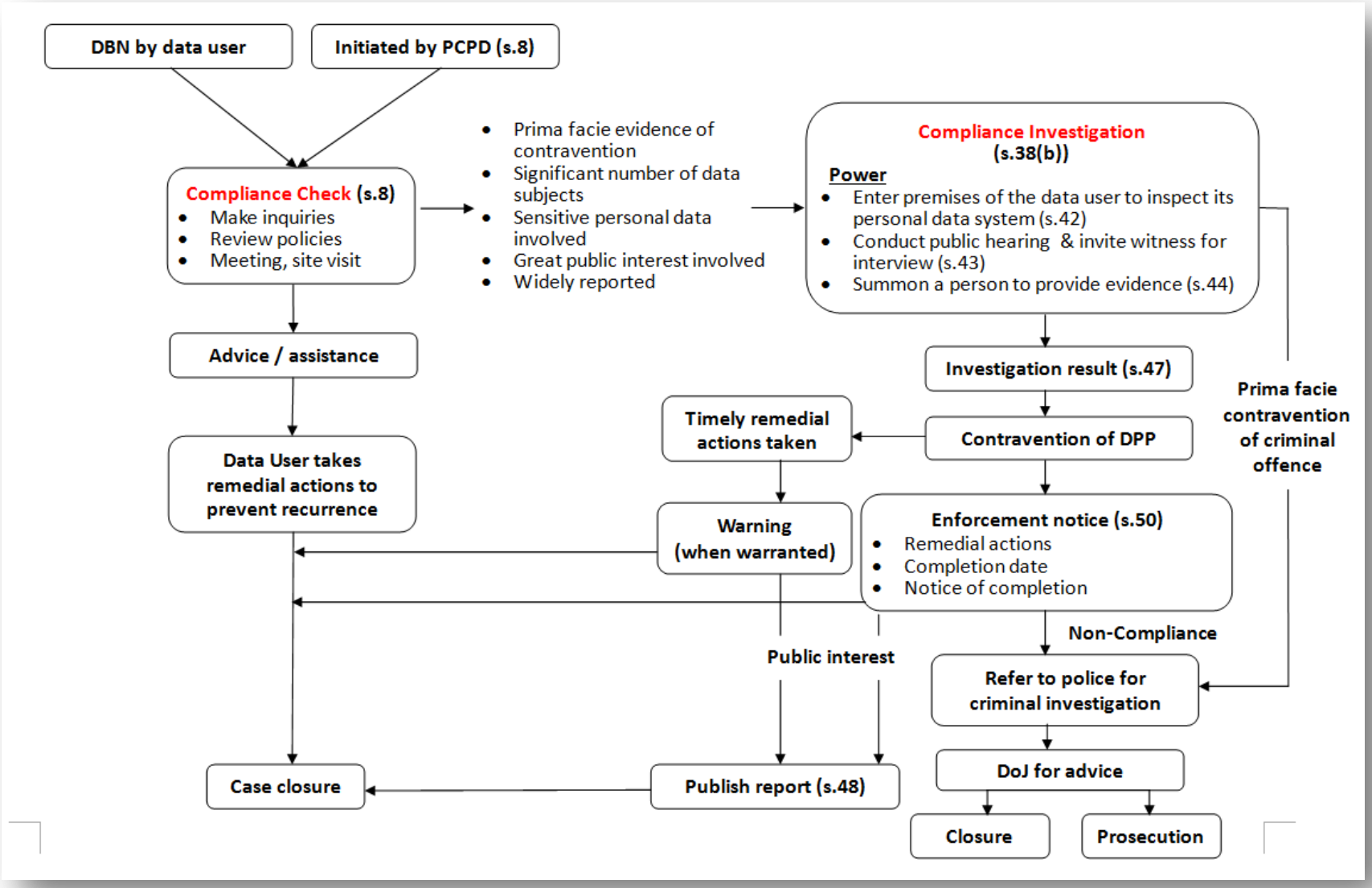
Enforcement Powers

Obstruction to the exercise of the Privacy Commissioner's investigation power is a criminal offence.

Handling of Complaints



Handling of Data Breaches & Compliance Investigations



Enforcement Powers

Enforcement Actions

- Serve enforcement notice on the relevant data user directing the data user to remedy, and if appropriate, prevent any recurrence of the contravention
- Non-compliance with an enforcement notice is a criminal offence (maximum fine HK$50,000 and imprisonment for 2 years, and a daily fine of HK$1,000 in case of a continuing offence)

Criminal Investigation and Prosecution

- The Privacy Commissioner does not have criminal investigation power
- Referral to the Police for criminal investigation and prosecution by the Department of Justice where appropriate

Remedies for Breach

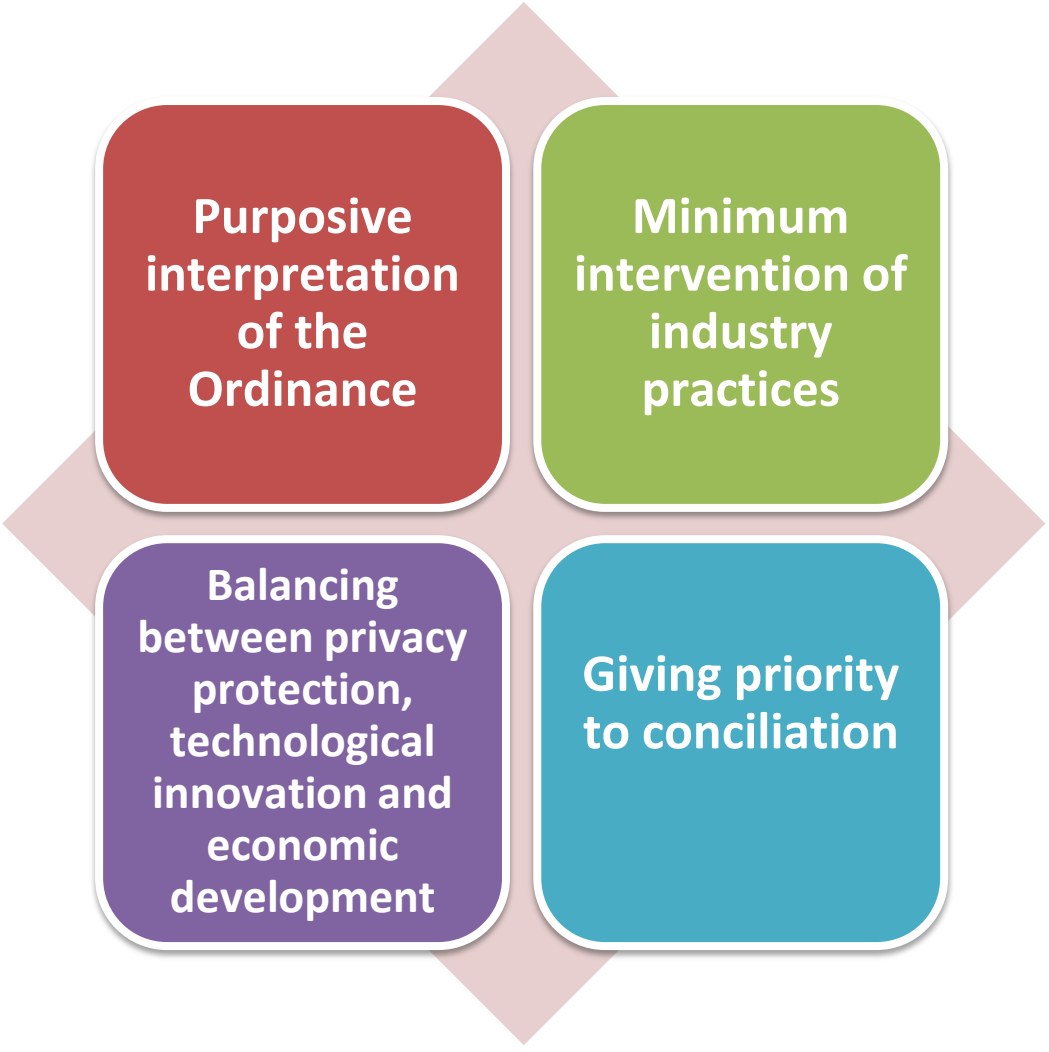
Civil Claims for Compensation

- An individual who suffers damage, including injury to feeling, by reason of a contravention of the Ordinance in relation to his personal data, is entitled to obtain compensation from the data user concerned

- The Privacy Commissioner may grant legal assistance to the aggrieved individual

4 Privacy Implications of Cloud and Big Data

Regulatory Approach



Cloud Computing and Personal Data Privacy

Bottom Lines

Personal Data Protection in the Cloud

Characteristics :

- Rapid cross-border data flow
- Rapidly changing / Loose outsourcing arrangements
- Standardised contracts adopted by the cloud service providers

Challenges:

- Unknown/or little control over data storage location
- How to assess whether the overseas data protection law offers comparable protection to the PDPO
- How can the same level of protection be assured
- How to explain to customer the risk of storing data overseas
- Whether there is subcontracting arrangements by the cloud provider
- Whether subcontractor observe the same terms and conditions as the cloud provider

Actions:

- Data user needs to know storage locations, have consent, ensures comparable law, or exercises due diligence etc.
- Cloud service provider needs to be transparent on outsourcing practice and have sufficient controls in place
- Ensure requirements are addressed in contract and enforced

Cloud Computing and Personal Data Privacy

- **Information leaflet issued by PCPD**

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

Cloud Computing

This information leaflet aims to advise organisations on the factors they should take into account in considering engaging cloud computing. It explains the relevance of the Personal Data (Privacy) Ordinance (the "Ordinance") to cloud computing. It highlights the importance for a data user to fully assess the benefits and risks of engaging cloud computing and understand the implications for safeguarding personal data privacy.

What is Cloud Computing?

There is no universally accepted definition of cloud computing. For the purpose of this leaflet, it is referred to as a pool of on-demand, shared and configurable computing resources that can be rapidly provided to customers with minimal management efforts or service provider interaction. The cost model is usually based on usage and rental, without any capital investment.

Cloud Computing Engagement and the Ordinance

Big Data

- **Massive scale of collection, processing, combination and aggregation of unstructured data**

Privacy Concerns of Big Data

Covert & ubiquitous collection of data

Unfairness & discrimination

Unpredictable / unexpected use of data

Profiling

Re-identification

Challenges of Internet of Things (IoT)

Vulnerability to hacking of IoT devices

- Unlike conventional computers, IoT devices (e.g. fitness bands, smart utility meters) may lack security hardware and software (e.g. no encryption applied to data, no firewall)
  - May be susceptible to hacking and data breach
  - May become launch pads for cyber attacks (e.g. distributed denial of service (DDoS) attack by using Botnet)

Sensitivity of data stored in IoT devices

- IoT devices may collect or infer intimate information about data subjects, e.g.:
  - Fitness bands → collect data about health conditions of data subjects, like heart rate, daily exercise level
  - Smart utility meter → infer habits and lifestyle of data subjects from their usage of utilities, like when to come home, when to go to bed

Principles for Use of Big Data

Characteristics of HK data protection law:

- principle-based
- technology-neutral

6 Data Protection Principles apply to use of Big Data and AI, e.g.,

- data security
- transparency
- use limitation

Challenges to the Data Protection Principles brought by Big Data and AI:

- excessive collection
- notice fatigue
- no genuine choice or meaningful consent

Possible Solutions:

De-identification

Accountability

Digital Ethics

- Beneficial
- proportionate
- respect
- fair and just

- Publicly available personal data is still subject to use limitation
- Exemption to use of personal data in statistics and research

5 Privacy Management Programme (PMP)

Accountability - data protection as part of corporate governance

- Privacy Management Programme launched in 2014
- Encourages organisations to embrace personal data privacy protection as part of their corporate governance responsibilities
- Apply as a top-down business imperative throughout the organisation
- Have in place appropriate policies and procedures that promote good practices

From Compliance to *Accountability*

Paradigm Shift

Compliance approach	Accountability approach
• Passive • Reactive • Remedial • Problem-based • Handled by compliance team • Minimum legal requirement • Bottom-up	• Active • Proactive • Preventive • Based on customer expectation • Directed by top-management • Reputation building • Top-down

PMP Best Practice Guide - Fundamental Principles

3 Top-down Organisational 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

PMP Best Practice Guide - Fundamental Principles

7 Practical Programme Controls

1. Personal Data Inventory	2. Policies	3. Risk Assessment Tools
4. Training & Education	5. Breach Handling	6. Data Processor Management
7. Communication		

PMP Best Practice Guide - Fundamental Principles

2 Review Processes

1

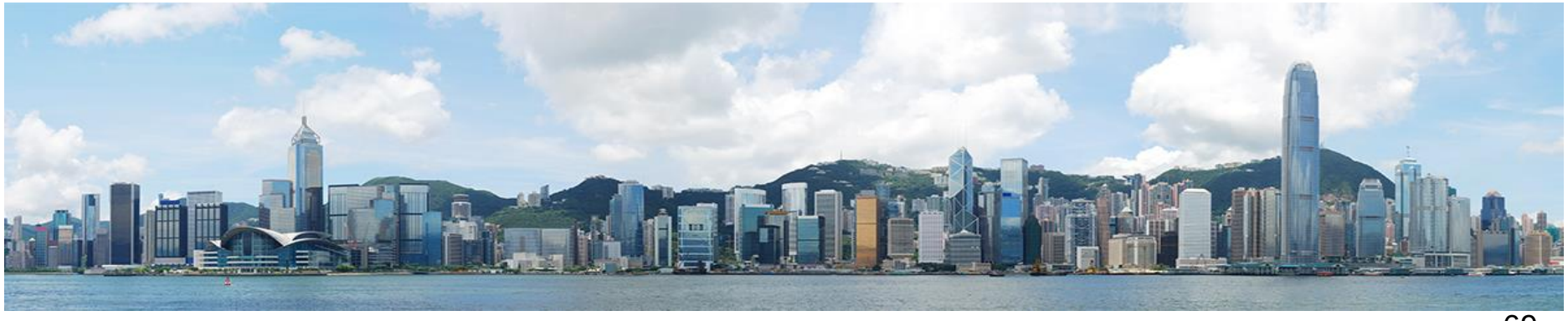
Develop an oversight review plan to check for compliance and effectiveness of the privacy management programme

2

Execute the oversight review plan making sure that any recommendations are followed through

私隱管理系統
Privacy Management Programme

Organisational Accountability - Example in Hong Kong



Participation in the PMP

Organisations pledged to implement PMP in Hong Kong:

- **All 76 bureaux and departments of Hong Kong Government**
- **25 insurance companies**
- **9 telecommunications companies**
- **5 organisations from other sectors**

Government Consultancy Project on Implementation of PMP

- Consultant engaged to facilitate bureaux/departments to implement PMP
- Advice provided by PCPD
- PMP Manual complied by the consultant
- PMP training to be provided by the consultant to government bureaux and departments

Practical Difficulties Encountered by Government Bureaux/Departments

Insufficient resources for DPO

e.g., finance, man power

Unfamiliar with new concepts

e.g., PIA, personal data inventory

Inconsistencies between PMP Manual and other Gov't guidelines

e.g. requirements for data security

6 Insurance Claims Database

Proposed Centralised Insurance Claims Database

Purpose:

- **Fraud detection and prevention**

Overarching principle:

- **Benefits of fraud detection must be balanced against data privacy rights**

Contains both historical and new data under 4 categories:

- **claims information, personal information, policy information and third party information**

Gist:

- **Is there a pressing need for data sharing?**

Proposed Centralised Insurance Claims Database

Data privacy issues:

Data collection

- Must be necessary for or directly related to fraud detection purpose; not excessive – DPP1(1)
- Notification on data sharing – DPP1(3)

Data accuracy and retention

- Data must be accurate for its purpose of use – DPP2(1)
- Date not kept longer than necessary – DPP2(2)
- Indefinite retention needs to be justified

Proposed Centralised Insurance Claims Database

Data privacy issues (con'd):

Data use

- **Prescribed consent** required for using historical data – DPP3(1)
- **Crime, etc exemption** applies? – s.58(2) → Prejudice test
- Cross-border transfer (access from overseas)?

Data security

- Take **reasonably practicable steps** to protect data from unauthorised or accidental access, processing, erasure, loss or use – DPP4(1)

Proposed Centralised Insurance Claims Database

Data privacy issues (con'd):

Data security (cont'd)

- Examples of appropriate security measures:
  - Data center based in Hong Kong
  - Certified information security system
  - Physical security measures
  - Limited access (need-to-know)

Transparency of policy

- Personal data policy and practices must be made known to public – DPP5

Proposed Centralised Insurance Claims Database

Data privacy issues (con'd):

Data access and correction rights

- Part 5 of PDPO & DPP6
- Mechanism for individuals to challenge analysis

7 Engagement with Stakeholders and the Public

Communications and Education

Communications and Education

1. Develop and implement promotion and public education programmes;
2. Identify, build and maintain amicable relationship with the media, interest groups and other stakeholders;
3. Foster partnership and collaborate with stakeholders on joint promotional campaigns/programmes e.g. trade associations;
4. Manage day-to-day communications and operational functions to include publications, print and electronic media; and interface with the public

Media & Communications

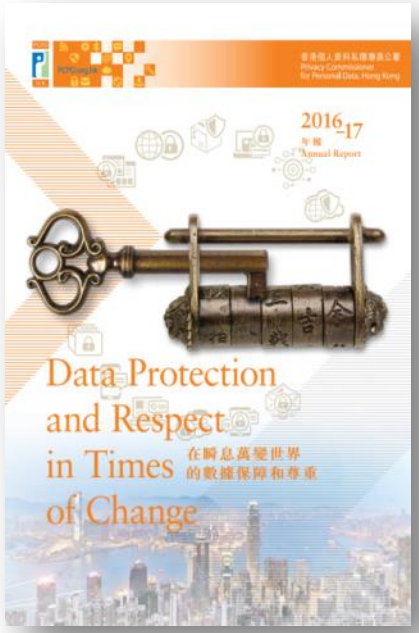
Media & Communications – Media Relations

In 2017, the PCPD:

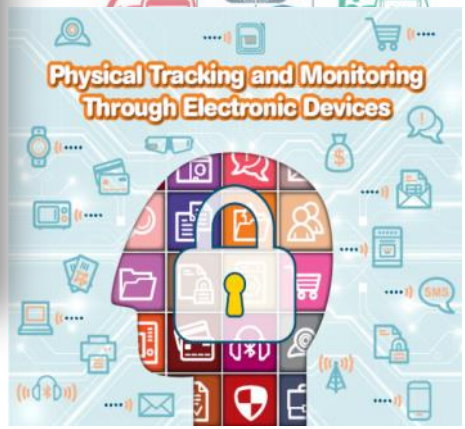
- **issued 30 media statements**
- **responded to 217 media enquiries**
- **gave 54 media interviews**

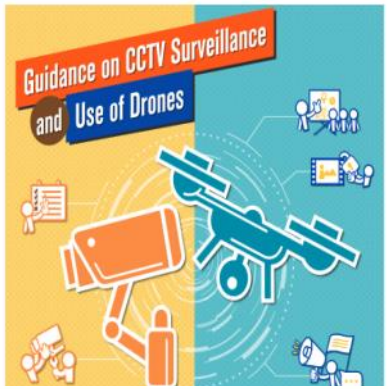
Media & Communications – Publications

The PCPD published and revised 13 publications in 2017

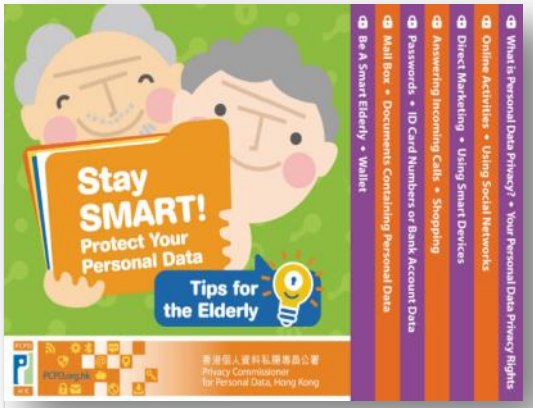


Annual Report



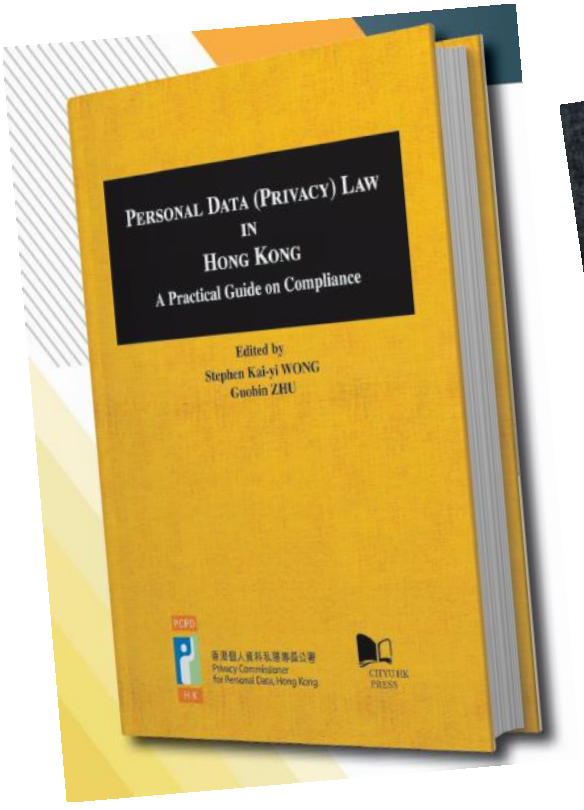


ICT-related



General

Media & Communications – Books



The Merit Award of "Mono / Duotone Color Book" Group under "Book Printing" Category of the 29th Hong Kong Print Awards 2017

Media & Communications – PCPD's website (www.pcpd.org.hk)

Received Silver Award for 2015 and 2016

Media & Communications – PCPD's website

US Web Marketing Association: 2015 Government Standard of Excellence Award

The WMA is proud to present this

2015 WEBAWARD FOR OUTSTANDING ACHIEVEMENT

in Web Development

WINNING ENTRY: Homepage of Office of the Privacy Commissioner for Personal Data, Hong Kong

WINNER NAME: Office of the Privacy Commissioner for Personal Data, Hong Kong

AWARD: Government Standard of Excellence

Media & Communications – Thematic Websites

www.pcpd.org.hk/besmartonline/

www.pcpd.org.hk/childrenprivacy

Media & Communications – Thematic Websites

ICDPPC Global Privacy and Data Protection Awards "Use of online tools" award: "Be SMART Online" thematic website enhancement

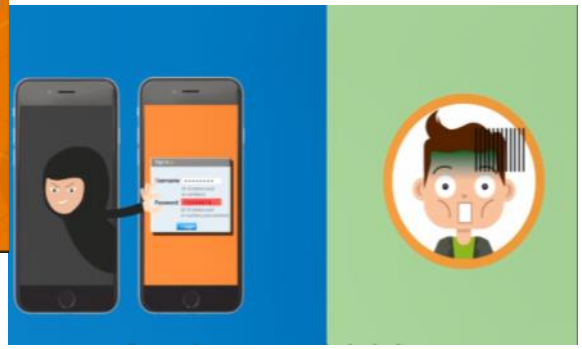
Other Online Communications – Social Media

www.youtube.com/user/PCPDHKSAR

www.facebook.com/besmartonlinepcpd

Promotion And Public Education: TV API And Educational Videos

PCPD launched a new TV Announcement in the Public Interest entitled "Think Privacy! Be Smart Online" and a series of four educational videos, calling on members of the public to go online vigilantly and protect, respect others' personal data



Education & Training

Promotion and Public Education: Professional Workshops, Seminars, Talks and Meetings with Stakeholders

- 314 professional workshops, seminars, talks and meetings were conducted in 2017 for a broad range of stakeholders
- attracted more than 25,000 participants from over 430 organisations

Education & Training - Professional Workshops and Seminars

- Professional Workshops and seminar:
  - ❒ Practical Workshop on Data Protection Law
  - ❒ Data Protection in Human Resource Management
  - ❒ Data Protection and Data Access Request
  - ❒ Data Protection in Banking/Financial Services
  - ❒ Data Protection in Insurance
  - ❒ Data Protection in Direct Marketing Activities
  - ❒ Privacy Management Programme
  - ❒ Recent Court and Administrative Appeals Board Decisions
- Introductory Seminars on the PD(P)O

Education & Training - Age-specific Activities (Youth Programme)

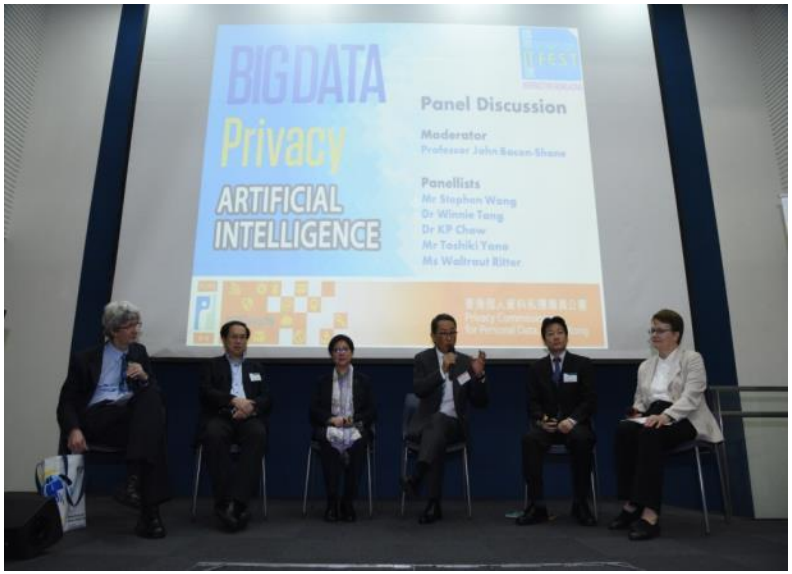
Student Ambassador Programme – 132 school partners

Education & Training - Age-specific Activities (the Elderly)

Education & Training
Topic-specific

Introduction to the European Union's General Data Protection Regulation

"Big Data, Artificial Intelligence and Privacy" Seminar



Education & Training - Industry Specific Campaign

- Hotel Industry
- Real Estate Industry
- Medical Practitioners in Public Hospitals
- Insurers
- Telecommunications
- Property Management Industry
- Retail Industry
- Mobile App Developers
- SME

Education & Training - Data Protection Officers' Club

- Established in February 2000
- Over 550 members from public and private sectors
- Serves as a platform for members to share and exchange views
- Activities include seminar, sharing session, visit etc.

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

Education & Training - Data Protection Officers' Club


DPOC e-newsletter

Issue 19, 9 October 2017

What's On

A fruitful finale to the 39th International Conference of Data Protection and Privacy Commissioners ("ICDPPC") hosted by the Privacy Commissioner for Personal Data, Hong Kong ("PCPD") from 25 to 29 September 2017

The 39th ICDPPC was successfully held from 25 to 29 September 2017 at Kowloon Shangri-La, Hong Kong. With the theme "Connecting West with East in Protecting and Respecting Data Privacy", the Conference has brought together more than 750 representatives from Data Protection Authorities ("DPAs"), policy makers, government and business leaders, information and communications technology ("ICT") professionals as well as academia and privacy advocates from over 60 countries or regions to Hong Kong.

The five-day Conference consisted of Closed Session (26 to 27 September 2017) for the ICDPPC members and observers, and Open Session (28 to 29 September 2017) attended by all in the data protection community.

The 39th International Conference of Data Protection and Privacy Commissioners

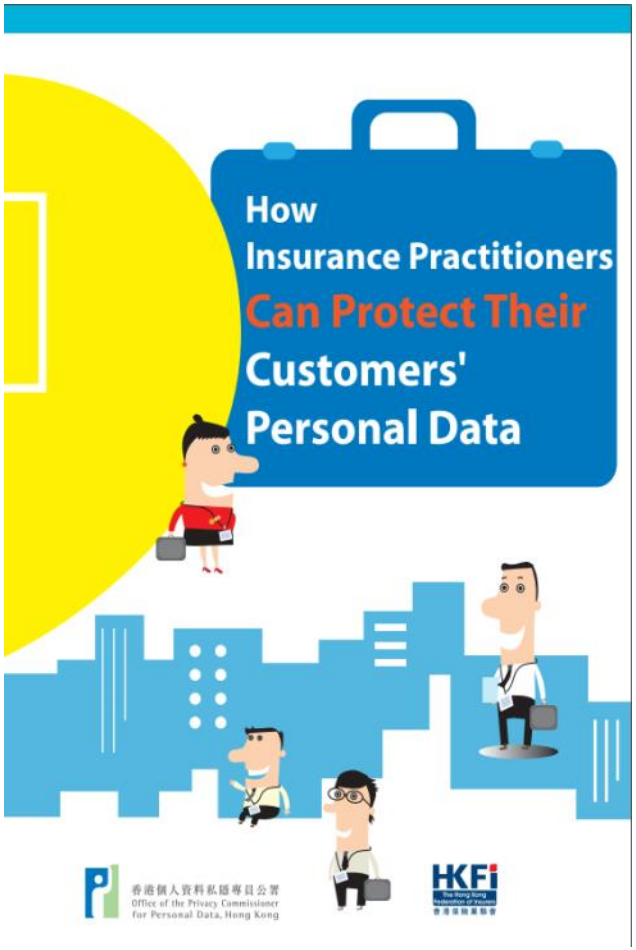
25-29 September 2017 | Kowloon Shangri-La, Hong Kong, China

Closed Session

At the Closed Session, in-depth discussions among the accredited members of ICDPPC focused on the issues of government information sharing. Speakers shared their views on the drivers and barriers to government information sharing, how it could trigger public concerns about discrimination and protection of sensitive information, and what was to be done.

During the Conference period, 26 side events were also staged by some 30 corporations and organisations from different sectors of the community, covering a wide range of privacy and data protection topics from global perspectives.

Education & Training - Training Materials and Multimedia assessment tools



Promotion & Projects

Promotion and Public Education: Major Activities

	2013	2014	2015	2016	2017
Major promotion and education activities	16	20	20	18	17
Total number of participants	58,979	141,443	260,223	193,260	258,147

Promotion & Projects – Promotional Events

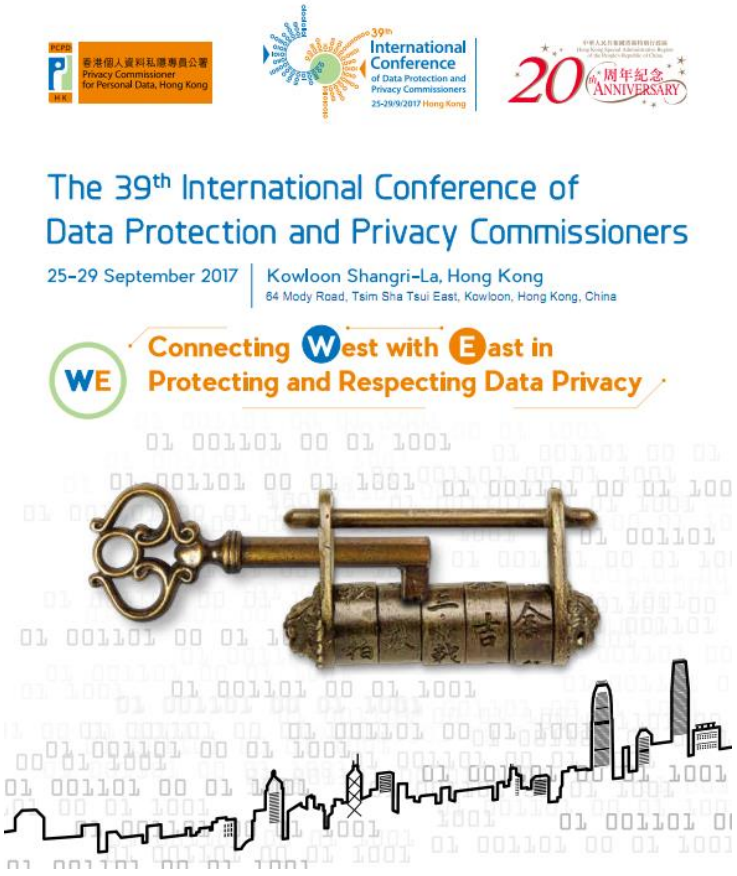
Public Education Roadshow

Public Seminars

Posters

The 39th International Conference of Data Protection and Privacy Commissioners

- **Connecting West with East in Protecting and Respecting Data Privacy**
- **More than 750 participants from Hong Kong and over 60 countries or regions attended**



The 39th ICDPPC

Sponsored Feature

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

The 39th International Conference of Data Protection & Privacy Commissioners
25–29 September 2017, Hong Kong, China

39th International Conference of Data Protection and Privacy Commissioners 25-29/9/2017 Hong Kong

20th 周年紀念 ANNIVERSARY

West Meets East in Protecting and Respecting Data Privacy

This world-class annual conference only twice convened in Asia since it was first held in 1979 – both times in Hong Kong and were 18 years apart. On this occasion, it was also to commemorate the 20th anniversary of the establishment of the Hong Kong SAR. The 39th International Conference of Data Protection & Privacy Commissioners (ICDPPC) convened in Hong Kong from September 25th to 29th, gathering more than 750 representatives from Data Protection Authorities, business leaders, ICT professionals and academics from over 60 countries or regions to exchange views and to promote the development of international standards on protection of personal data. After his appointment in 2015, Privacy Commissioner for Personal Data, Hong Kong Stephen Kai-yi Wong took on the challenge of hosting the event as one of his important goals "to showcase the developments arising from technology and data evolutions in the mainland of China as well as other Asian countries".

The ICDPPC was first convened in 1979 in Germany, and the conferences in the first 20 years were primarily held in European locations. Hong Kong became the first jurisdiction in Asia to have a comprehensive piece of legislation on personal data privacy and an independent Privacy Commissioner for regulatory work when the Personal Data (Privacy) Ordinance (Cap 486) (the Ordinance) came into force in 1996 and the Privacy Commissioner for Personal Data, Hong Kong (PCPD) was established in the same year as an independent statutory body to oversee the enforcement of the Ordinance.

The PCPD actively follows up on complaints from members of the public to ensure data users, from public or private sector, comply with the Ordinance. In addition, it is moving beyond enforcement to broader engagement with stakeholders through promotion and public education. Wong shared that the success of the "Clean Hong Kong Campaign" is a good demonstration on how preventive efforts can go hand in hand with prohibitive measures in achieving goals. The PCPD is investing an increasing amount of resources in educational programmes, organising classes and seminars for members of the public as well as professional practitioners to cultivate the culture of protect and respect data privacy.

An important topic of the conference is the European Union's impending implementation of its General Data Protection Regulation (GDPR) next year, which will impose substantial financial penalty on corporate offenders. Given the diversified business or transaction models (e.g. online transactions), it is important for businesses in Hong Kong to ascertain if the GDPR is applicable to them, and to keep up with the new changes. The PCPD will publish guidance and organise seminars to help local organisations and professionals better understand the GDPR and its application. It is also noted that organisations in Hong Kong are generally wary of negative publicity generated by infringement of the Ordinance that can impugn their goodwill and reputation. It provides a powerful incentive for compliance, and paves the way for the PCPD to work closely with businesses in Hong Kong in formulating internal guidelines and best practices in data protection.

Advancement in technology, rapid growth in online activities, and ubiquity of the mobile platform have all aggravated the threat to privacy and the risk of personal data abuse. Alternative strategies were suggested by speakers and panellists at the conference to address the challenges arising from deployment of technologies that has led to the rise of data analytics and use of "Big Data" enabled by widespread collection and processing of personal data. "Accountability" and "transparency" were offered as models of good corporate governance to complement the "notice and consent" process – which mirror the ethical approach of building "trust and respect" advocated by the PCPD as well as Data Protection Authorities worldwide. Wong said data users should do more than just complying with the regulations, and an "equitable" data privacy right should be developed for all stakeholders.

With increasing reliance on ICT as the backbone of growing international trade and other exchanges, the volume of international data flows has escalated exponentially. The demand generated by China's Belt and Road Initiative (BRI) will only exacerbate the trend. Because of its strength in the free flow of information, its protection of freedoms and human rights, and its data protection law and framework, Hong Kong is well poised to become the data hub for the BRI within one country but outside the jurisdiction of the mainland of China, facilitating transfer and storage of data, connecting and converging ideas and information between the mainland of China and the rest of the world.

During the conference, winners of the ICDPPC Global Privacy and Data Protection Awards were also announced, including the PCPD's "Be SMART Online Thematic Website Enhancement" project that won the "Use of Online Tools" category award. Guests of Honour and speakers for the conference included the Honourable Rimsky Kwok-keung Yuen (GBM, SC, JP, Secretary for Justice, Government of the Hong Kong SAR), the Honourable Patrick Tak-kuen Nip (JP, Secretary for Constitutional and Mainland Affairs, Government of the Hong Kong SAR), and the Honourable Charles Peter Mok (JP, Member of the Legislative Council – Information Technology, Hong Kong SAR).

> **"Usually, after these conferences I can think of more to add to my list of 44 suggestions for conference organisers but on this occasion, I cannot think of any additional points"**
>
> **Stewart Dresner**, Chief Executive, Privacy Laws & Business

> **"That was a real pleasure for me to work together with you and your team. The bar for the next ICDPPC Organising Committee was set really on high level"**
>
> **Wojciech Rafal Wiewiorowski**, Assistant Supervisor, European Data Protection Supervisor

> **"In my 30 years of career in HSBC, I have attended numerous conferences locally and in overseas', and I have to say that this is one of the most remarkable and impressive conferences that I have ever attended – contents, logistic arrangements, hospitality of the organizers, location ...., are all first class!"**
>
> **Thomas C M Yung**, Head of Data Protection, The Hongkong and Shanghai Banking Corporation Limited

Privacy Commissioner Stephen Kai-yi Wong delivering a speech at the 39th ICDPPC

The Guest of Honour and Secretary for Justice of Hong Kong SAR, The Honorable Rimsky Kwok-keung Yuen delivering the opening speech at the 39th ICDPPC

A full house of participants

Chairperson of the ICDPPC John Edwards presenting an award to Privacy Commissioner Stephen Kai-yi Wong

Many thanks to our sponsors and supporting organisations!

Sponsors:

facebook · Microsoft · OneTrust Privacy Management Software · 蚂蚁金服 ANT FINANCIAL · Google · intel

八達通 OCTOPUS · MAYER·BROWN JSM · DataGuidance · iapp · ISMA · Alibaba Group · CLP 中電 · MTR · NYMITY · VISA

Supporting organisations:

Constitutional and Mainland Affairs Bureau
Correctional Services Department
Department of Justice
Electronic Health Record Office, Food and Health Bureau
Hong Kong Tourism Board
Innovation & Technology Bureau
Invest Hong Kong
Office of the Communications Authority
Office of the Government Chief Information Officer
Trade and Industry Department

The supporting organisations below are arranged in alphabetical order by organisation name

Chinese Executives Club of Hong Kong Management Association
City University of Hong Kong
Committee on the Promotion of Civic Education
Communications Association of Hong Kong
Consumer Council
DLA Piper Hong Kong
Estate Agents Authority
Federation of Hong Kong Industries
French Association of Personal Data Protection Authorities
Hogan Lovells
Hong Kong Institute of Arbitrators Council
Hong Kong Institute of Certified Public Accountants
Hong Kong Institute of Human Resource Management
Hong Kong Mediation Centre
Hong Kong Monetary Authority
HongKong Airlines
Information Systems Audit and Control Association (ISACA), China Hong Kong Chapter
Mandatory Provident Fund Schemes Authority
PC Woo & Co
Sidley Austin
The American Chamber of Commerce in Hong Kong
The Asian Academy of International Law
The Chinese Manufacturers' Association of Hong Kong
The Hong Kong Association of Banks
The Hong Kong Computer Society
The Hong Kong Federation of Insurers
The Hong Kong General Chamber of Commerce
The Hong Kong General Chamber of Small and Medium Business
The Hong Kong Institute of Bankers
The Hong Kong Institute of Chartered Secretaries
The Hong Kong Institution of Engineers
The Law Society of Hong Kong

The 39th ICDPPC

The 39th ICDPPC

The 39th ICDPPC


THANK YOU !

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