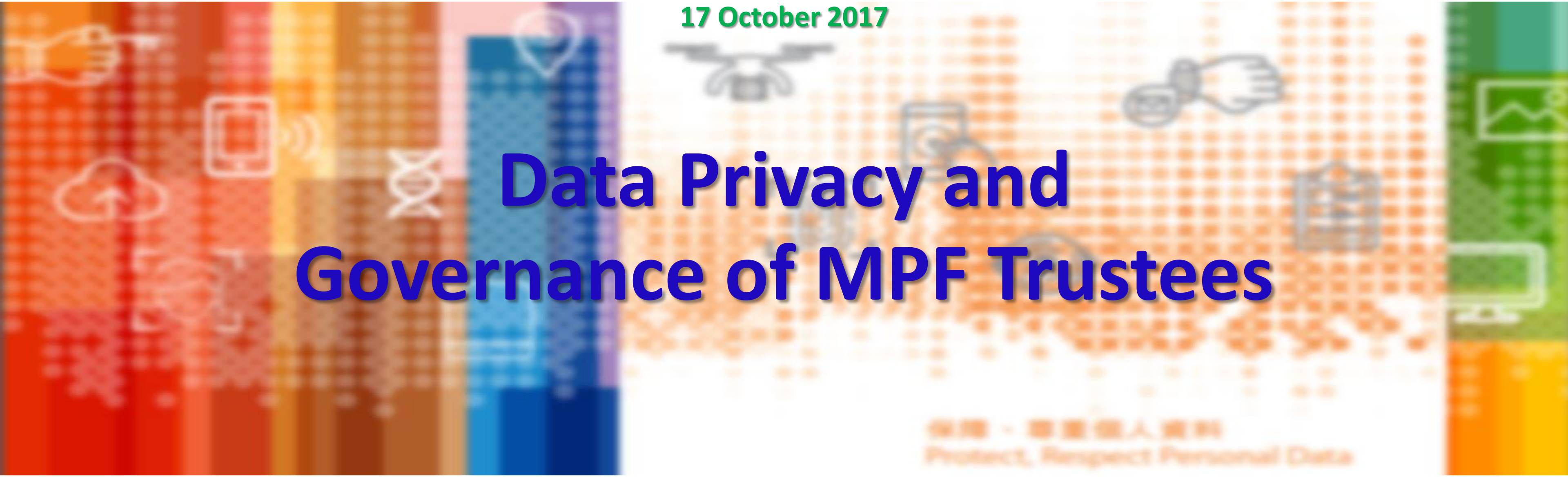
Workshop on Governance of MPF Trustees

Mandatory Provident Fund Schemes Authority

Auditorium, 56/F, Two International Finance Centre, Central

17 October 2017



Data Privacy and Governance of MPF Trustees

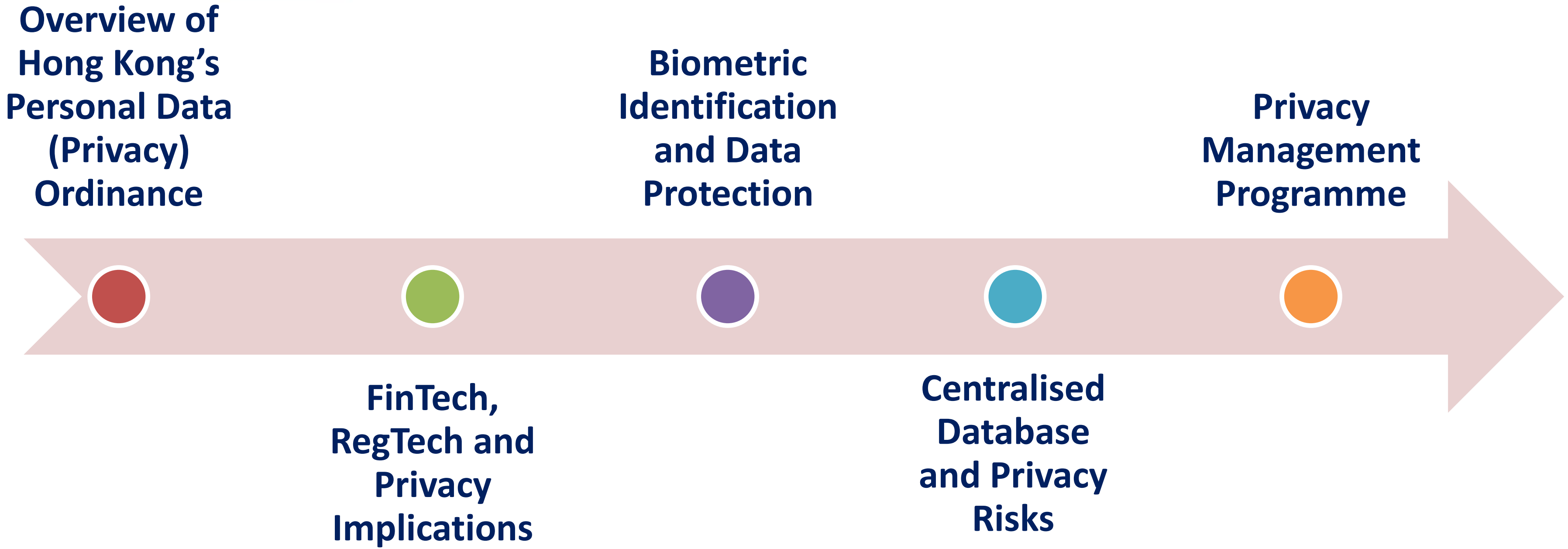
Stephen Kai-yi Wong, Barrister

Privacy Commissioner for Personal Data, Hong Kong

PCPD
HK
PCPD.org.hk
est.1996

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

Presentation Outline



- Overview of Hong Kong's Personal Data (Privacy) Ordinance
- FinTech, RegTech and Privacy Implications
- Biometric Identification and Data Protection
- Centralised Database and Privacy Risks
- Privacy Management Programme

An Overview of
The Personal Data (Privacy) Ordinance

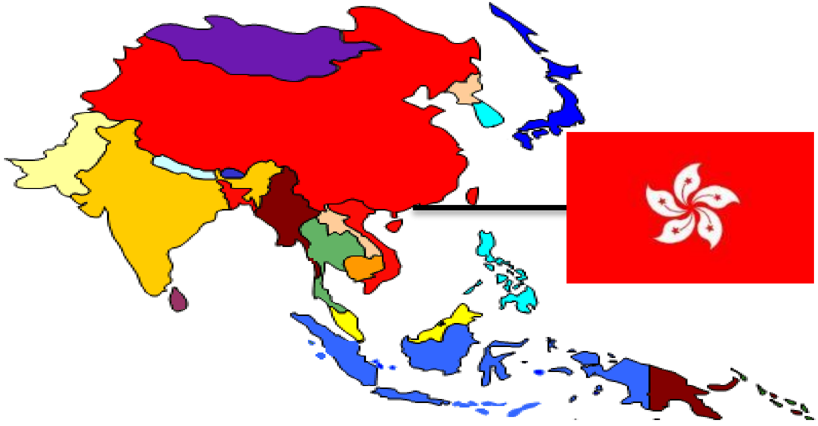
Legislative Intent

- **Business Perspective** – To facilitate business environment, maintain Hong Kong as a financial and trading hub

- **Human Rights Perspective** – Protect individuals' personal data privacy

Personal Data (Privacy) Ordinance

- enacted in **1995**
- **1st** 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**



What is “Personal Data”?

“Personal data” (個人資料) means any data -

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

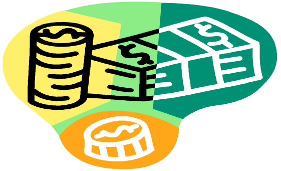
(b) *from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and*

(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*****.**

Examples of Personal Data in Everyday Life

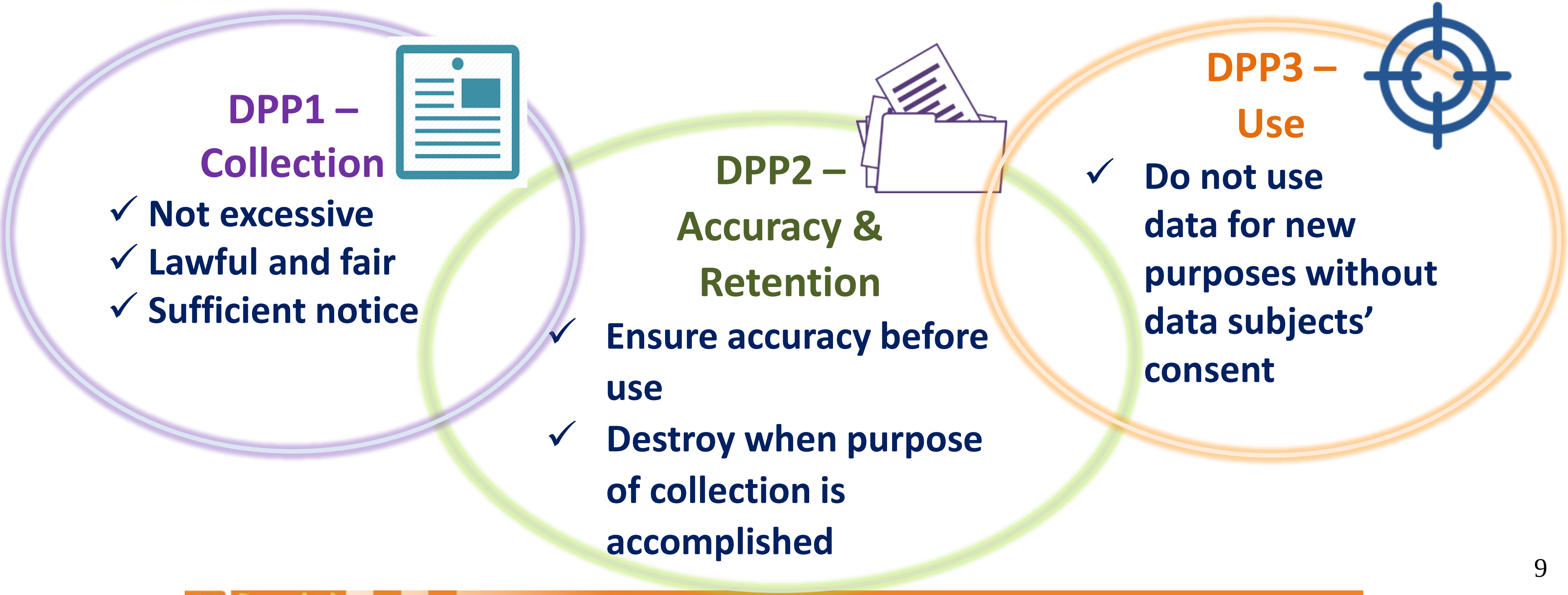
- a person’s name, telephone number, address, sex, age, occupation, salary, nationality, photo, identity card number, medical records, etc.



Six Data Protection Principles (DPPs)

- **Core spirits** of the Ordinance
- Cover **the whole data lifecycle** from collection, retention, use, security to destruction

Six Data Protection Principles (DPPs)



DPP1 – Collection

- ✓ Not excessive
- ✓ Lawful and fair
- ✓ Sufficient notice

DPP2 – Accuracy & Retention

- ✓ Ensure accuracy before use
- ✓ Destroy when purpose of collection is accomplished

DPP3 – Use

- ✓ Do not use data for new purposes without data subjects’ consent

Six Data Protection Principles (DPPs)

DPP4 – Security

✓ All practicable steps shall be taken to prevent data breach

DPP5 – Openness & Transparency

✓Policy and practice should be made readily available to data subjects

DPP6 – Data Access & Correction

✓Allow data subjects to access and correct their personal data

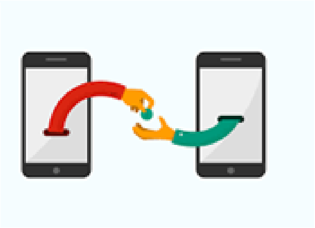
FinTech, RegTech and Privacy Implications

FinTech

- **Application of technology in financial services:**

E-wallet

Crowdfunding



P2P Lending

Robo-Adviser

Credit Scoring

RegTech

- Application of technology for regulatory and compliance purposes:

By Regulators:
Use of Big Data analytics and machine learning to track down irregular stock transactions

By Market Practitioners:
Use of Big Data analytics and machine learning to identify money laundering activities

FinTech and RegTech

Collection of Big Data, e.g. E-wallet

Use of Big Data Analytics, e.g. Credit scoring

Use of Online Platform (e.g. Cloud) to store, process and transmit data

Examples of RegTech for Compliance

1 *Regulatory reporting*
Regulatory reporting through Big Data analytics, real time reporting and cloud

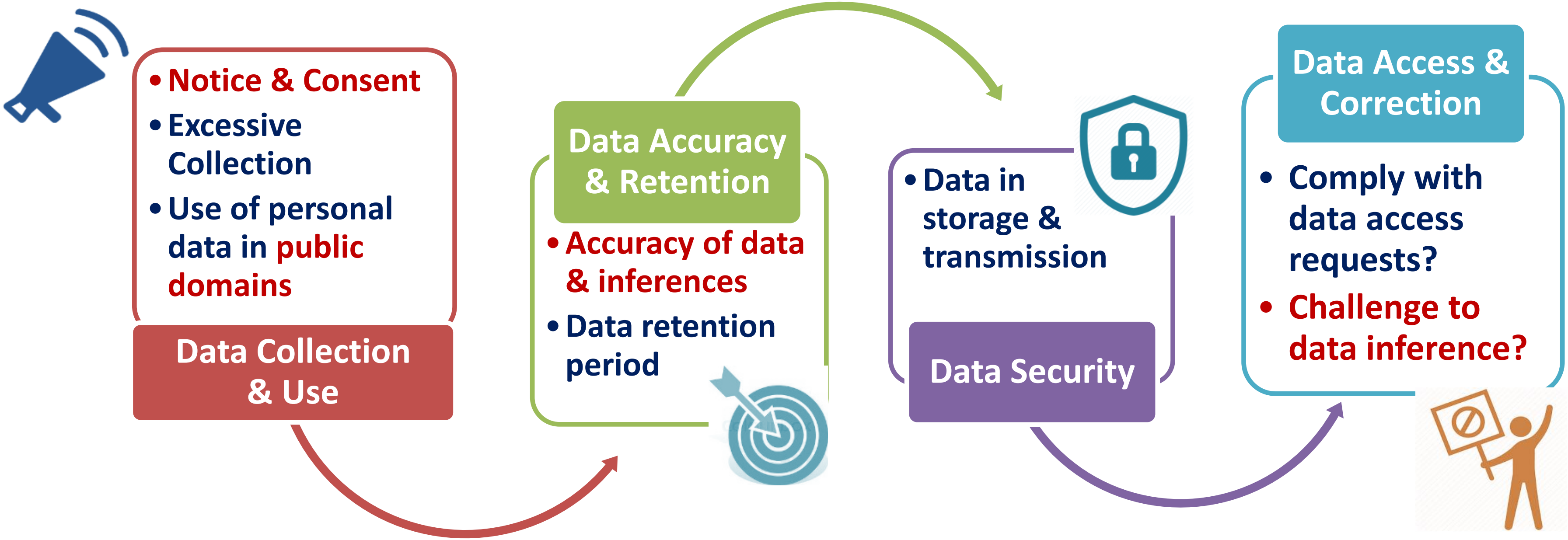
2 *Risk Management*
Detect compliance and regulatory risks, assess risk exposure and anticipate future threats

3 *Identity Management & Control*
Facilitate counterparty due diligence and Know Your Customer procedures. Manage consent for use of personal data

4 *Compliance*
Real time monitoring and tracking of current state of compliance and upcoming regulations

Source: Deloitte

FinTech and RegTech – Privacy Implications



Data Collection & Use

- Notice & Consent
- Excessive Collection
- Use of personal data in public domains

Data Accuracy & Retention

- Accuracy of data & inferences
- Data retention period

Data Security

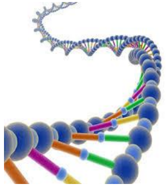
- Data in storage & transmission

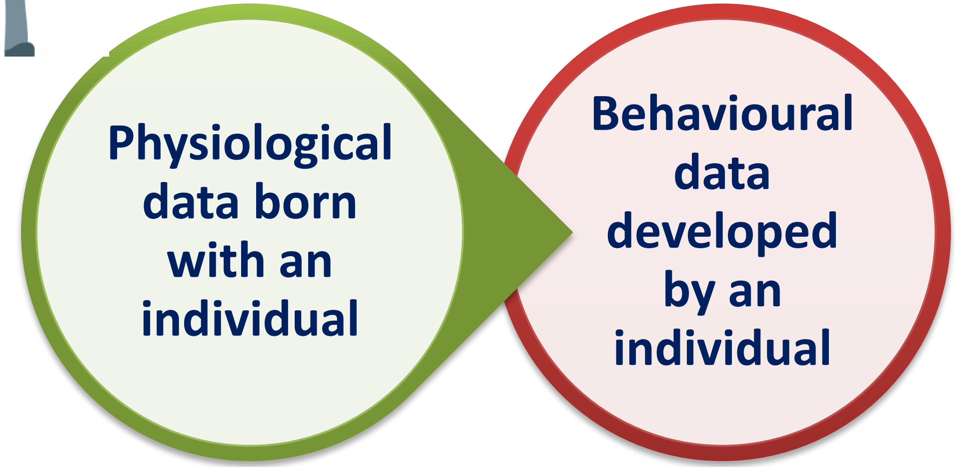
Data Access & Correction

- Comply with data access requests?
- Challenge to data inference?

Biometric Identification and Data Protection

Biometric Data





Physiological data born with an individual

Behavioural data developed by an individual

- DNA, fingerprint, palm veins, iris, retina, facial images and hand geometries

- hand writing pattern, typing rhythm, gait, voice

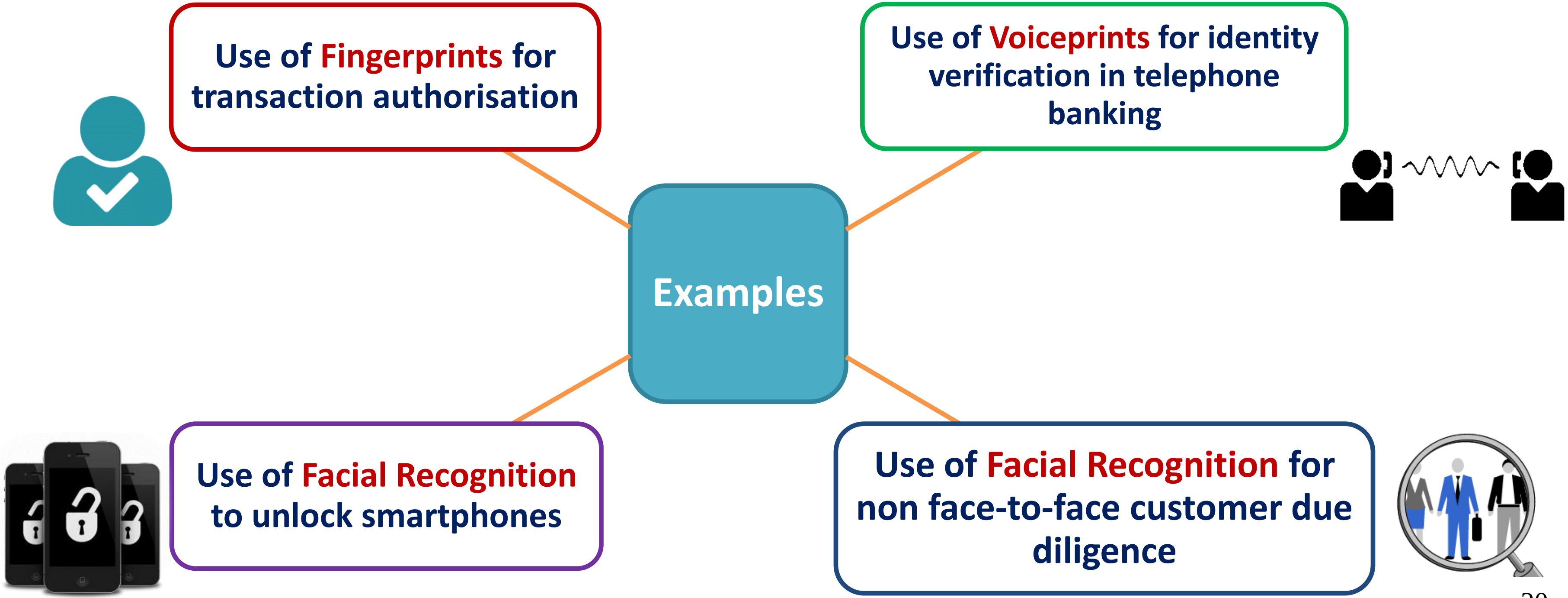
Is Biometric Data Personal Data?

- does it belong to an individual?
- does it identify an individual?
- if *both* are ‘Yes’, then biometric data is personal data

or

- biometric data alone (e.g. fingerprint) may not reveal identities
- biometric data in a database that links customers/staff members is personal data

Biometric Identification



Examples

Use of **Fingerprints** for transaction authorisation

Use of **Voiceprints** for identity verification in telephone banking

Use of **Facial Recognition** to unlock smartphones

Use of **Facial Recognition** for non face-to-face customer due diligence

Why Protect Biometric Data?

Uniqueness – The more unique, the more certain of the identity

- DNA
- Fingerprint
- Hand geometry
- face
- hand writing
- gait

Permanence

- once leaked, forever leaked – unlike passwords - one cannot change his fingerprints or DNA after leakage
- consequences - lead to identification, impersonation, identity theft, misuse…

Why Protect Biometric Data?

Inference

- DNA, retina, vein pattern may reveal the ethnic, health and mental conditions of individuals
- implication – discrimination in selection process such as employment, offering of insurance, etc.

Multipurpose: If biometric data can be used for more than just identification

- face (race)
- fingerprint (criminal record)
- palm vein (physical health conditions)
- retina (physical health conditions)
- DNA (physical and mental health conditions, probability of diseases)

Impact on Individuals

Risk Factors	DNA	Fingerprint	Facial images	Handwriting pattern	Hand geometry
1. Uniqueness	High	High	Medium	Low	Low
2. Any likely changes with time	No	No	Yes	Yes	Yes
3. Multiple purposes	Yes	Yes	Yes	No	No
4. Covert collection	Yes	Depends	Yes	Unlikely	No
5. Impact on individuals	Grave	High	Some	Some	Small

Biometric Data – Case Sharing (1)

- A fashion trading company collected **employees' fingerprint data** for (i) **monitoring staff attendance** and (ii) **office security**

- **Commissioner's Findings – Excessive and Unfair collection:**
  - Excessive:
    - Company already had sufficient security measures in place, e.g. CCTV cameras, digital locks, chain locks
    - Company only had 20 employees, staff attendance could be effectively monitored by less privacy intrusive means
  - Unfair:
    - Employees were not given any choices at all

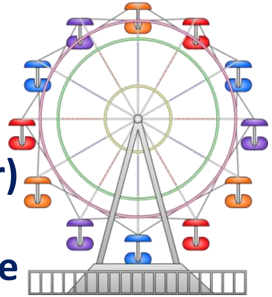
Biometric Data – Case Sharing (2)

- A school collected **fingerprints of its staff and pupils** for (i) **recording attendance** and (ii) **provision of lunch and library services**

- **Commissioner's Findings – Excessive collection:**
  - ○ **Children** of school age or individuals incapable of managing their own affairs are **vulnerable, warranting greater protection** of their privacy
  - ○ Consent not free from **undue influence**, given the special relationship between the school and its pupils and between the school and its staff
  - ○ The purposes of recording attendance and provision of lunch and library services could be achieved by other **less privacy intrusive alternatives**

Biometric Data – Case Sharing (3)

- An amusement park collected visitors' fingerprint for multiple-entry tickets



- **Commissioner's Findings – No Contravention:**
  - Purpose of collection: verify the identity of a ticket holder (i.e. visitor) without having to inspect his identification document
  - Only a code generated from the visitor's fingerprint was stored in the theme park's system.
    - No image of fingerprint was retained
    - The code was stored in encrypted form
    - Not practicable for the park to link up the code with that particular visitor
    - The code would be deleted once the ticket expired
  - The visitor could freely opt for other means of verification, like registering his/her name on the ticket, and such option was informed to the visitor

Protection of Biometric Data

1. Need for a Privacy Impact Assessment

- The need for collecting biometric data
- Whose biometric data should and could be collected
- The extent of the data to be collected

2. Justifications for Collecting and Using Biometric Data

- What is the purpose of collection and how is data collected?
- Is collection for a lawful purpose directly related to the organisation's function and activity? Necessary and not excessive?
- Identification vs. Verification

Protection of Biometric Data

3. **Risk Minimisation Techniques** in biometric data collection

- Keep the templates of the biometric data, rather than the original samples

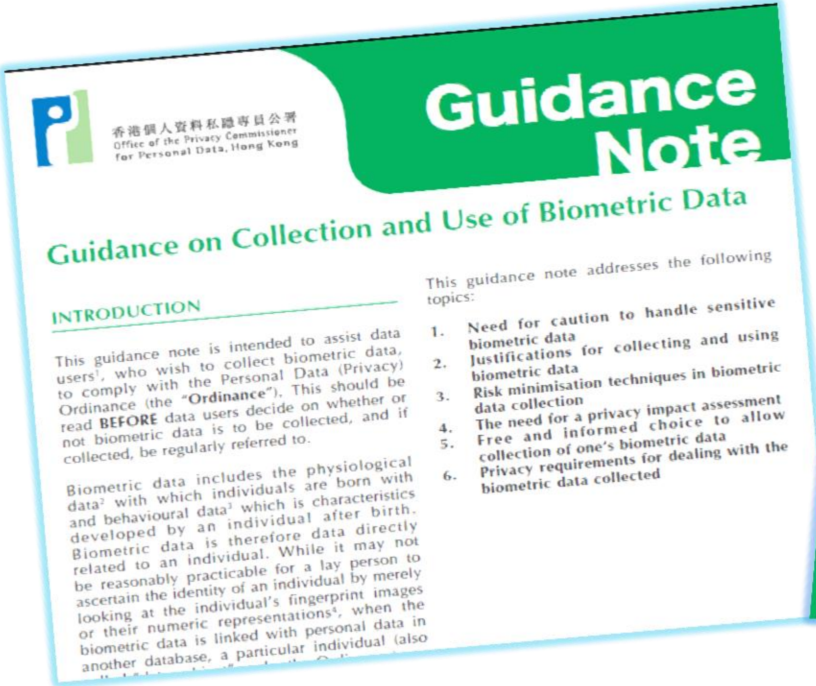
4. **Free and informed choice** to allow collection of biometric data

- Provide less privacy intrusive alternative if possible
- Full explanation of privacy impact of collection
- Fair collection

5. **Need for Caution** in handling biometric data

- Establish strong controls
- Data retention
- Data accuracy
- Secondary use
- Data security
- Make privacy policy available
- Staff trainings

PCPD’s Publications



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 Collection and Use of Biometric Data

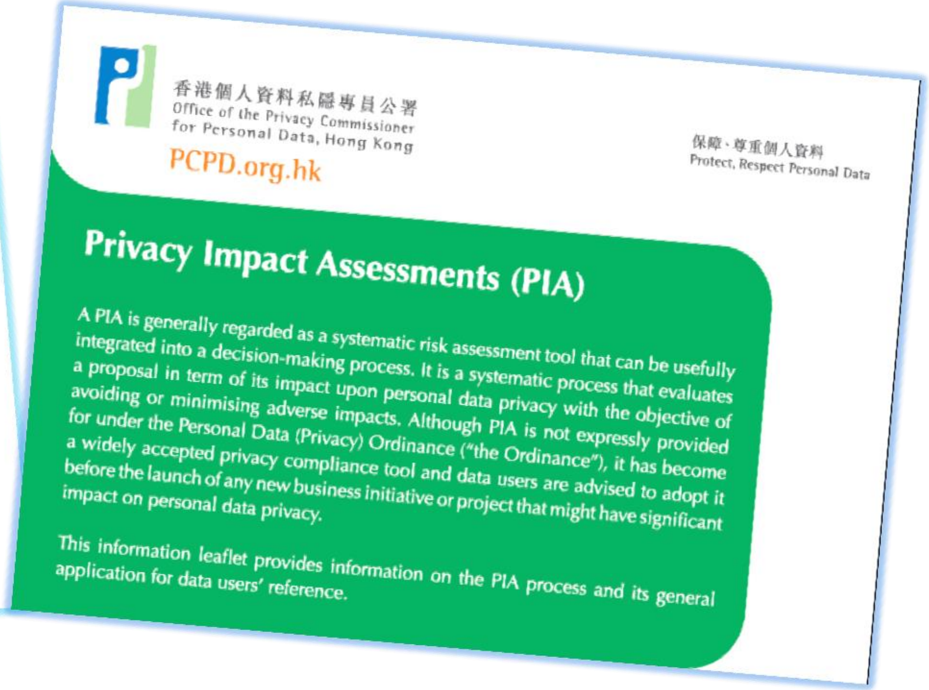
INTRODUCTION

This guidance note is intended to assist data users[1], who wish to collect biometric data, to comply with the Personal Data (Privacy) Ordinance (the “**Ordinance**”). This should be read **BEFORE** data users decide on whether or not biometric data is to be collected, and if collected, be regularly referred to.

Biometric data includes the physiological data[2] with which individuals are born with and behavioural data[3] which is characteristics developed by an individual after birth. Biometric data is therefore data directly related to an individual. While it may not be reasonably practicable for a lay person to ascertain the identity of an individual by merely looking at the individual’s fingerprint images or their numeric representations[4], when the biometric data is linked with personal data in another database, a particular individual (also

This guidance note addresses the following topics:

1. **Need for caution to handle sensitive biometric data**
2. **Justifications for collecting and using biometric data**
3. **Risk minimisation techniques in biometric data collection**
4. **The need for a privacy impact assessment**
5. **Free and informed choice to allow collection of one’s biometric data**
6. **Privacy requirements for dealing with the biometric data collected**



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 Impact Assessments (PIA)

A PIA is generally regarded as a systematic risk assessment tool that can be usefully integrated into a decision-making process. It is a systematic process that evaluates a proposal in term of its impact upon personal data privacy with the objective of avoiding or minimising adverse impacts. Although PIA is not expressly provided for under the Personal Data (Privacy) Ordinance (“the Ordinance”), it has become a widely accepted privacy compliance tool and data users are advised to adopt it before the launch of any new business initiative or project that might have significant impact on personal data privacy.

This information leaflet provides information on the PIA process and its general application for data users’ reference.

https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_biometric_e.pdf
https://www.pcpd.org.hk//english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

Centralised Database

Centralised Database Proposals – Hong Kong

Hong Kong Association of Banks: Centralised Know Your Client (KYC) Database

- **Enhance KYC process between multi-stakeholders for various purposes**
- **Reduce duplication and increase efficiency**
- **Enhance financial services by innovation via FinTech and Big Data**
- **Enhance data portability between banks**

Hong Kong Federation of Insurers: Centralised Insurance Claims Database

- **Help insurance companies detect fraudulent insurance claims and take early preventive measures**
- **Protect interests of policy holders**

Centralised Database – Overseas Experiences

Sweden

- In 2003, 6 major Swedish banks developed **BankID** as an electronic identification used to access public and private services.

Singapore

- In 2016, Singapore government launched **MyInfo**, a centralised database of citizens, permanent residents and foreigners.
- In April 2017, 4 banks accept bank account opening applications via MyInfo without additional documents.

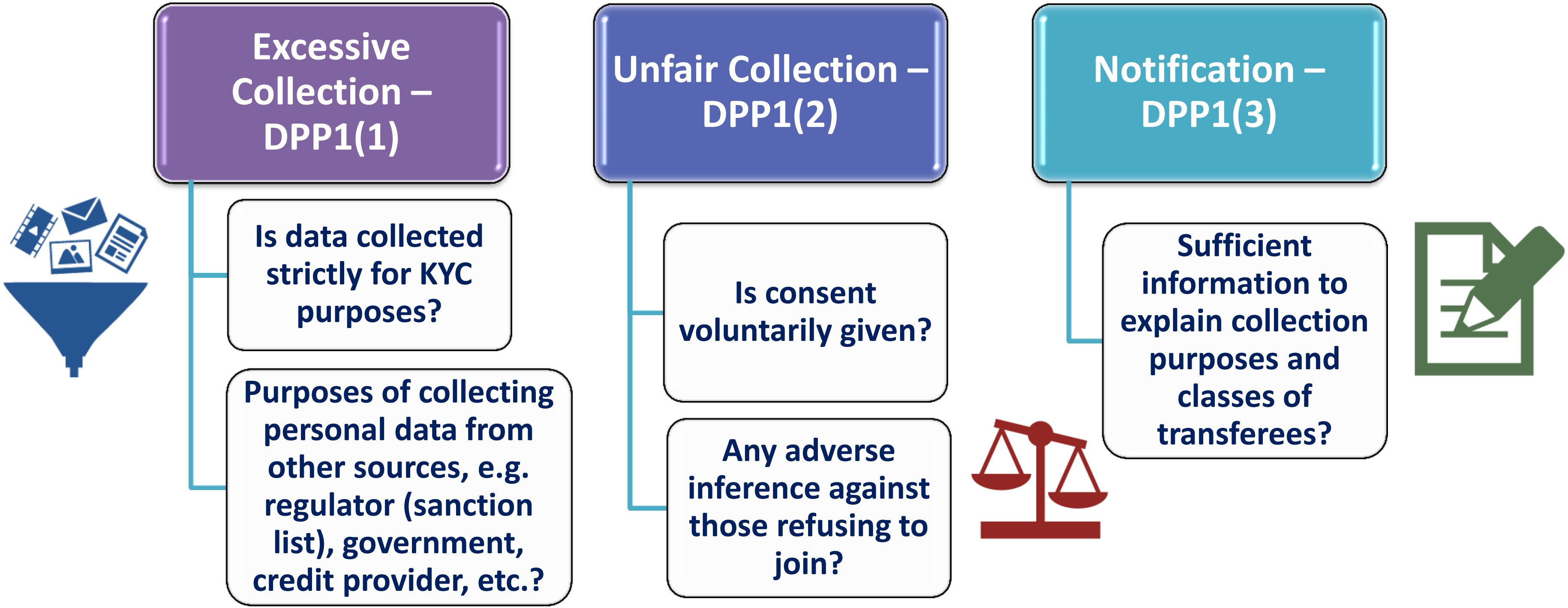
United Kingdom

- UK Government collaborated with the banking sector to establish KYC database.
- **“GOV.UK Verify”** provides electronic identification and trusted login for all UK government digital services.

Philippines

- A bill for Philippines national ID system, **Filipino Identification System** or FilSys has just been approved by the House Committee on Population.
- Proof of identification for both public and private sectors.

Centralised Database – Privacy Risks



Excessive Collection – DPP1(1)

- Is data collected strictly for KYC purposes?
- Purposes of collecting personal data from other sources, e.g. regulator (sanction list), government, credit provider, etc.?

Unfair Collection – DPP1(2)

- Is consent voluntarily given?
- Any adverse inference against those refusing to join?

Notification – DPP1(3)

- Sufficient information to explain collection purposes and classes of transferees?

Centralised Database – Privacy Risks

Accuracy & Retention – DPP2(1) & (2)

- Steps to ensure data accuracy?
- How long is data retained?

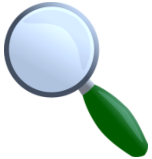
Use & Disclosure – DPP3

- Data used and disclosed strictly for KYC purposes?
- Who can access database and Why?

Security – DPP4

- All practicable steps to ensure security?

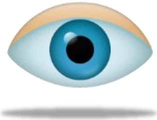
Transparency & Access/ Correction – DPP5 & 6



Centralised Database – Governance and Regulation

Who is the **data user** in control of the database?

What is the appropriate **governance** for the database?



What is the appropriate **regulatory approach**?

From Compliance, to Accountability… to

Main Objectives of PMP

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

Privacy Management Programme

A Best Practice Guide

Contents

Introduction	[2]
The Benefits of Implementing a Privacy Management Programme	[3]
Developing a Comprehensive Privacy Management Programme	[3]
Part A – Baseline Fundamentals of a Privacy Management Programme	[3]
Part B – Ongoing Assessment and Revision	[9]
Privacy Management Programme – At a Glance	[11]

- embrace personal data privacy protection as part of the corporate governance responsibilities; and
- apply it as a top-down business imperative throughout the organisation

https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf

From Compliance to Accountability

Paradigm Shift

Compliance approach

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

Accountability Approach

- Active
- Proactive
- Preventative
- Based on customer expectation
- Directed by top management
- Reputation building
- Top-down

PMP Best Practice Guide - Fundamental Principles

3 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

PMP Best Practice Guide - Fundamental Principles

7 Practical Programme Controls

1. Record and maintain personal data inventory
2. Establish and maintain data protection and privacy policies
3. Develop risk assessment tools (e.g. privacy impact assessment)
4. Develop and maintain training plan for all relevant staff
5. Establish workable breach handling and notification procedures
6. Establish and monitor data processor engagement mechanism
7. Establish communication so that policies and practice are made known to all stakeholders

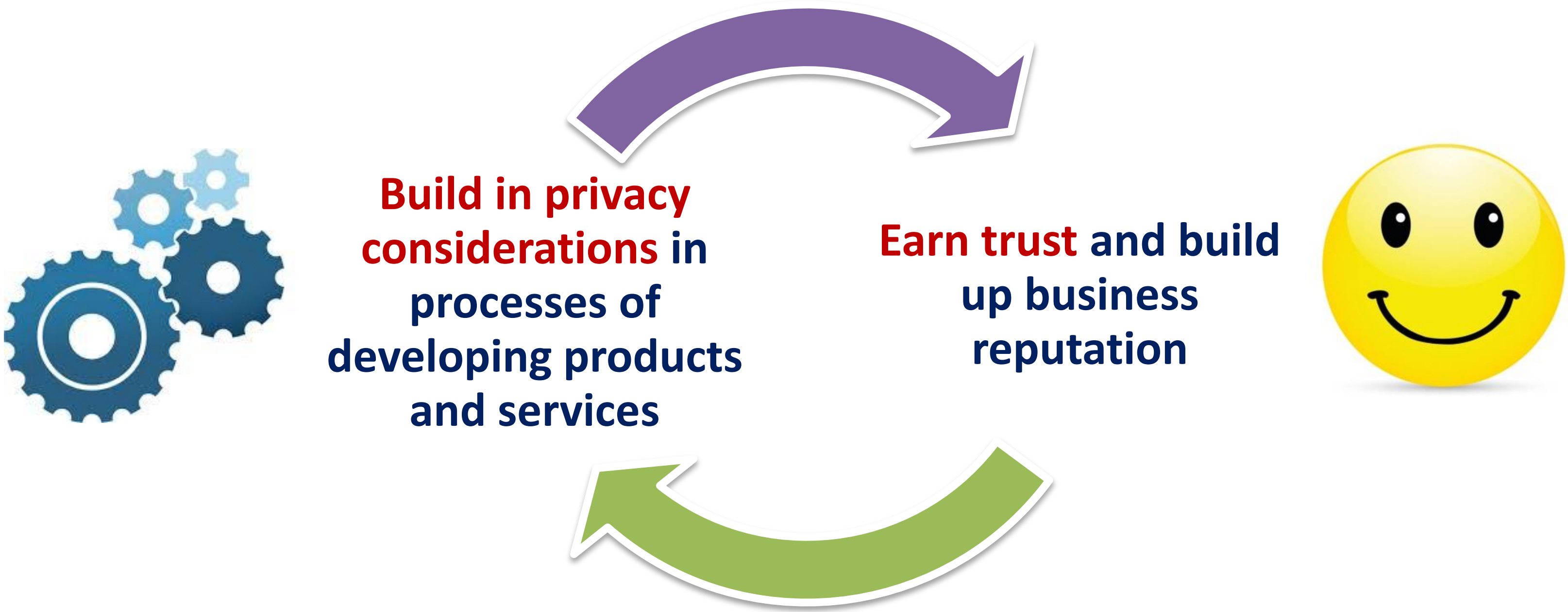
PMP Best Practice Guide - Fundamental Principles

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

Privacy by Design and by Default



Build in privacy considerations in processes of developing products and services

Earn trust and build up business reputation

Contact Us

PCPD
PCPD.org.hk
HK
香港個人資料私隱專員公署
Privacy Commissioner for Personal Data, Hong Kong
保障、尊重個人資料
Protect,Respect Personal Data
About PCPD | Data Privacy Law | News & Events | Compliance & Enforcement | Complaints | Legal Assistance | Education & Training | Resources Centre | Enquiry
A Quick Guide
Hot Search
Advanced Search
Keyword Search
RSS
A A A
The 39th International Conference of Data Protection and Privacy Commissioners
25-29 September 2017 | Kowloon Shangri-la, Hong Kong, China
WE
Connecting West with East in Protecting and Respecting Data Privacy
REGISTER NOW
20

The 39th International Conference of Data Protection and Privacy Commissioners (ICDPPC)

The 39th International Conference of Data Protection and Privacy Commissioners is now open for registration.

What's New

More

PCPD Wins the "Most Breastfeed-caring Corporate" Award

PCPD's New Chinese Publication Entitled《注意! 這是我的個人資料私隱》has been released at the Hong Kong Book Fair 2017! The new book sharing session was held at the HKCEC on 24 July 2017.

PCPD Publishes a New Book Entitled "Watch out! This is my personal data privacy" - Have a Say on Your Own Privacy! (Chinese version Only)

Privacy Commissioner Welcomes the Enactment of the Apology Ordinance

Organisations and Individuals Should Comply with Lawful Requirement of the Privacy Commissioner - A Company Director Became the First Offender Convicted of this Offence

Privacy Commissioner Publishes Investigation Report on the Loss of Registration and Electoral Office's Notebook Computers containing Personal Data of Election Committee Members and Electors

PCPD Joins Global Sweep Exercise to Examine Consumers' Control Over Their Personal Data Collected by Customer Loyalty and Reward Programmes

"It is a timely opportunity for Hong Kong to review the data privacy protection law" Privacy Commissioner Delivers Keynote Address at the 7th European Data Protection Days in Berlin, Germany

For Individuals

Think Privacy! Be Smart Online

Using Computers and the Internet Wisely

Be Smart on Social Networks

Your Identity Card Number and

For Organisations

Mobile App Development

Professional Workshops

Online Courses

Introduction to the PD(P)O Seminar

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

Copyright

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