

GSMA Policy Group Meeting

23 June 2019 | Harbour Grand Hong Kong

Privacy Issues in Digital Era and Data Ethics as the Solution

保護 - 尊重個人資料
Protect, Respect Personal Data

Stephen Kai-yi WONG, Barrister

Privacy Commissioner for Personal Data, Hong Kong

1

PCPD



HK



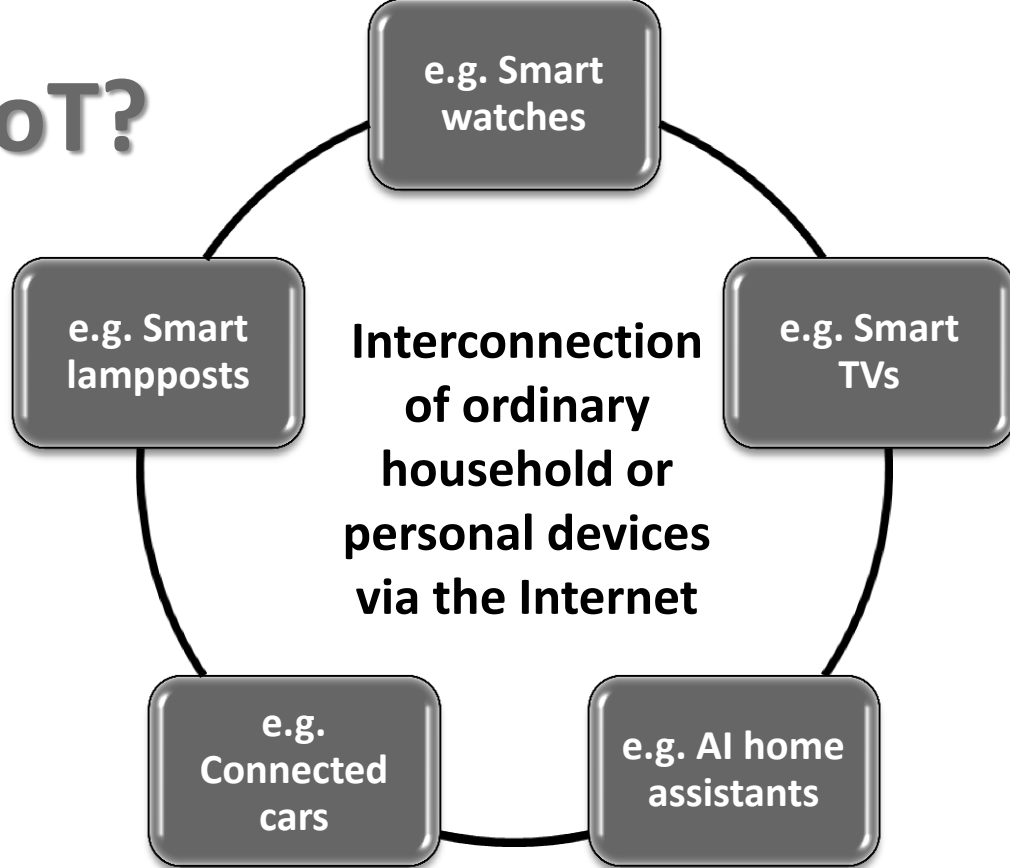
PCPD.org.hk

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



IoT

What is IoT?



IoT may involve one or more of the following technologies...

Examples of applications:

- Intelligent traffic signal
- Real-time parking vacancy system
- Smart lamppost
- Autonomous vehicle

Electronic sensor

RFID / NFC

Examples of applications:

- Mobile payment
- Electronic baggage tag
- Auto toll
- Electronic road pricing

Example of application:

- Almost everything

Wi-Fi / Mobile network

Webcam

Examples of applications:

- Real-time traffic information
- Electronic road pricing
- Smart lamppost
- Autonomous vehicle

Example of application:

- Autonomous vehicle

Audio recording

iBeacon

Examples of applications:

- Crowd management
- Smart lamppost

Whether the data collected by IoT is “personal data”?

Definition of “personal data” under the PD(P)O



(a) Relating directly or indirectly to a living individual



(b) Practicable for the identity of the individual to be directly or indirectly ascertained; and



(c) In a form in which access to or processing is practicable

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

5

Whether the data collected by IoT is “personal data”?

ability to collect a vast amount of intimate information concerning an individual’s health, movements, habits and private life

piecing together information gathered via different IoT devices → allow a profile be constructed of the IoT user

tracking of an IoT device may be tantamount to behavioural tracking of the user

Whether the data collected by IoT is “personal data”?



The US Court of Appeal
for the Seventh Circuit

*Naperville Smart Meter
Awareness v.
City of Naperville*, No. 16-3766
(7th Cir. 2018)

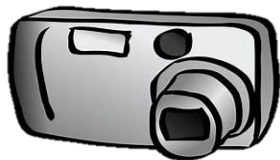
energy consumption data of a household collected by a smart energy meter

protected by the Fourth Amendment to the US Constitution (i.e. the right of people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures)

the energy usage data revealed information about the happenings inside the house

7

Meaning of “collect” as defined in *Eastweek* case applicable in the context of IoT?



The *Eastweek* case



A complaint lodged with the PCPD in 1997

The complainant was photographed by a magazine without her knowledge or consent

The photograph published in the magazine accompanied by unflattering and critical comments on her dressing style

Revisit the Meaning of “collect” as defined in *Eastweek* case in the context of IoT

The *Eastweek* case

PCPD: contravened
DPP 1(2)(b)

Court of Appeal:
No “collection” of
personal data by the
publisher

Court of First
Instance for judicial review:
Application dismissed

Revisit the Meaning of “collect” as defined in *Eastweek* case in the context of IoT

e.g. Individuals’ online activities unprotected

e.g. Burden on the individuals and regulators to prove the intent of the businesses

e.g. Images collected by CCTVs unprotected if no “collection” of personal data

Deprive individuals of PD(P)O protection

e.g. May subsequently identify individuals and reveal details of their intimate lives by applying techniques of big data analytics and profiling

e.g. Personal data collected and used for big data analytics and AI algorithms unprotected

Privacy Risks of IoT

An IoT device (e.g., webcam, iBeacon) may track, monitor and collect data from *any persons* coming within its monitoring area

Indiscrimination and excessive collection
(cf. DPP 1)

Covert tracking and monitoring; no meaningful notice and consent
[cf. DPPs 1 & 3]

Vulnerable to security breach
(DPP 4)

Individuals may be unaware of the tracking and monitoring devices (e.g. RFID, webcam, iBeacon)

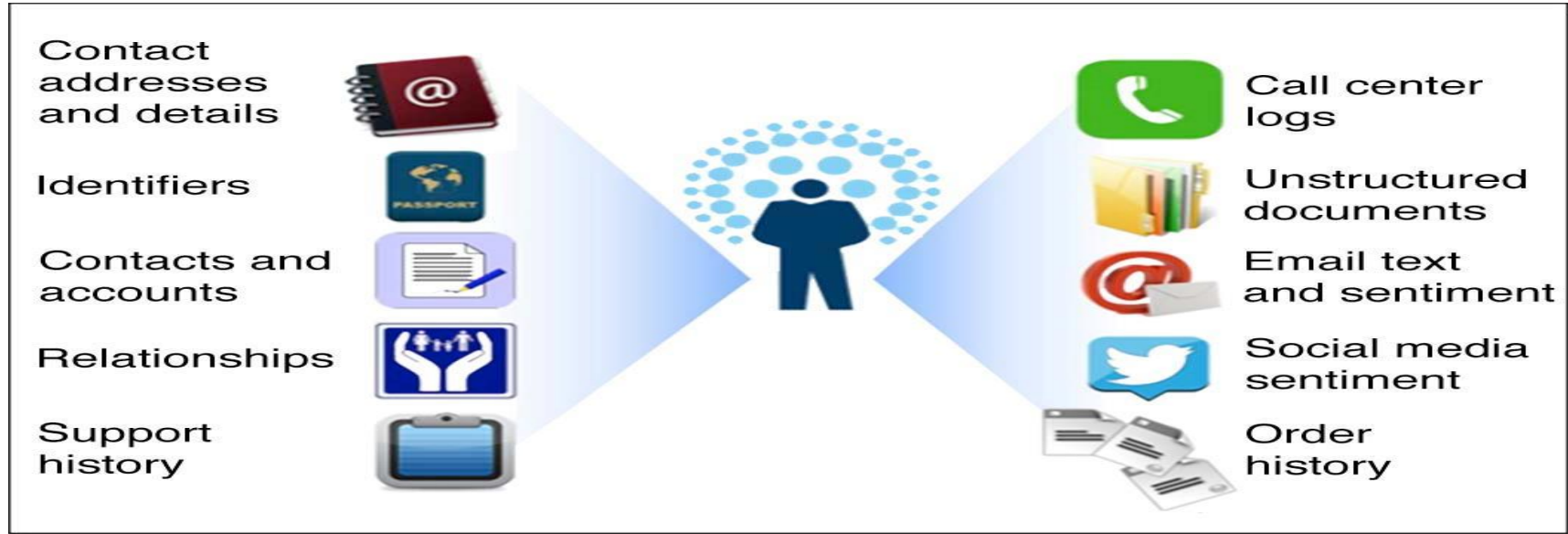
Privacy Risks

IoT devices may lack security measures (e.g., firewall, anti-virus software, end-to-end encryption)

11

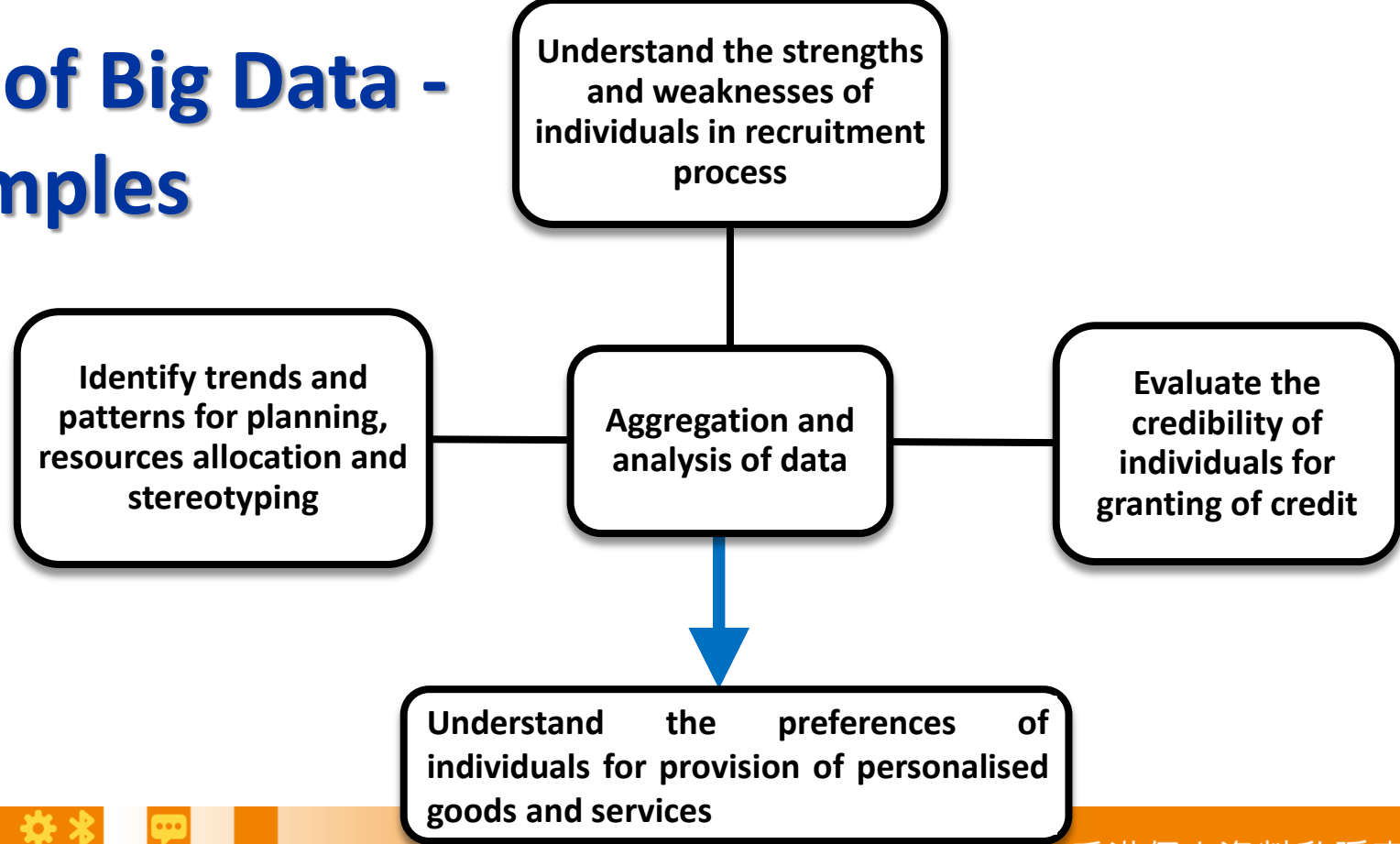
Big Data

Massive scale of collection, processing, combination and aggregation of structured & unstructured data



12

Use of Big Data - Examples



Privacy risks associated with open data and big data analytics

Open data / Big data analytics

- **Re-identification** of individuals from anonymous data by big data analytics [*cf. DPP 1 (fair collection)*]
- Revelation of **personal secrets** by big data analytics [*cf. DPP 1 (fair collection)*]
- Mistaking coincidence / correlation as causality → **bias / unfair discrimination** [*DPP 2 (accuracy)*]
- Sharing and use of personal data beyond individuals' **reasonable expectations** [*cf. DPP 3*]
- Lack of **transparency** (unexplainable algorithms) [*cf. DPP 5*]

14

Challenges of the Digital Revolution

**Ubiquitous collection
of data**

**Unpredictability in
use and transfer**

**Challenges global data
privacy frameworks
based on 'notice' and
'consent'**

**Cyber threats, attacks
and resilience**



Carpenter v. United States (2018)

- ❖ Police obtained 129 days' worth of cellphone location history from a phone company

The Supreme Court: Obtaining these records without a warrant violated Mr. Carpenter's rights

16

Challenges of the Digital Revolution

**Challenge for
regulator**



**Facilitate the
innovative use
of data within
the legal and
ethical
frameworks**



**Minimise the
privacy risks,
creating
healthy synergy
with economic
growth**



Regulatory Developments

18

PCPD



HK



PCPD.org.hk

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

Regulatory developments in response to Digital Revolution

OECD Guidelines 1980

Provided an international privacy framework

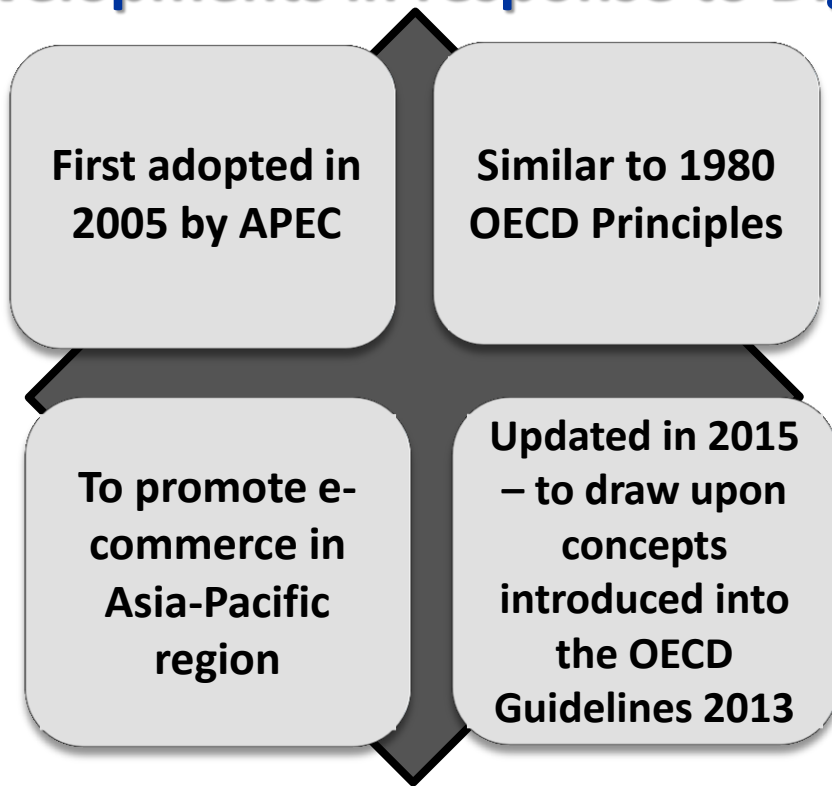
8 fundamental principles – now reflected in global privacy laws

Updated in 2013 to introduce, amongst others:

- data breach notification
- privacy management programme
- global interoperability

Regulatory developments in response to Digital Revolution

APEC Framework



Regulatory developments in response to Digital Revolution

1st Generation

1980 OECD Privacy Principles

– international privacy framework, in response to development in automatic data processing



2nd Generation

1995 EU Data Protection Directive

– model privacy concepts for EU national laws



3rd Generation

2016 GDPR

– 28 EU national privacy laws harmonised into one
– addresses challenges of rapid technological developments & globalisation

21

PCPD



HK



PCPD.org.hk

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

GDPR Main Objectives

One set of rules for all companies operating in the EU

People have more **control** over their personal data

Businesses benefit from a **level playing field**

GDPR

- Accountability

Measures to
ensure
compliance
[Art. 24]

Data
protection by
design and by
default
[Art. 25]

Data
Protection
Impact
Assessment
[Art. 35]

Data
Protection
Officer
[Art. 37]

Recent regulatory developments in Asia



Mainland
China

Slow-starter due to a different traditional culture on privacy

Fast catching up – in view of economic reform and urbanisation in 21st Century

No omnibus privacy law yet

- privacy regulation is scattered over various sets of rules and regulations

24

Privacy regulation is scattered over various sets of rules and regulations in the mainland of China

Law on the Protection of Consumer Rights and Interests
[2013 revised]

Cybersecurity Law
[1 June 2017 implemented]

“Security Assessment for Measures for Cross-Border Transfer of Personal Information and Important Data”
[2017 Draft]

“Personal Information Security Specification”
[1 May 2018 implemented]
[1 February 2019 proposed amendments]

General Rules of the Civil Law
[2017 revised]

“Guidelines for Data Cross-Border Transfer Security Assessment”
[2017 Draft]

“Guidelines on Protection and Security of Internet Personal Information”
[2019 released]

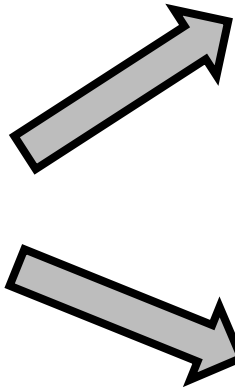
“Administrative Measures for Data Security”
[2019 Draft]

“Regulations on Network Protection of Minor’s Personal Information”
[2019 Draft]

“Measures on Security Assessment of Cross-Border Transfer of Personal Information”
[2019 Draft]

Recent regulatory developments in Asia

The Personal Information Protection Law under Category 1 on legislative agenda of the Standing Committee of the National People's Congress



conditions for legislation are mature

Bill will likely be deliberated within the current 5-year term of the Standing Committee

Recent regulatory developments in Asia

The Standing Committee has listed the formulation of the personal information protection law in its legislative plan, and relevant departments are working on it



Spokesperson for
the second session
of the 13th
National People's
Congress

27

PCPD



HK



PCPD.org.hk

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

Recent regulatory developments in Asia

Personal Data Protection Act (effective in 2006)

- Modelled on the Portuguese data protection regime, similar to 1995 EU Data Protection Directive

Macao, China

Cybersecurity Law (amended the draft made in April 2019), applies to-

- public sectors' networks and data systems; and
- private entities that operate critical infrastructures (e.g. transportation, telecommunication, health, banking, electricity)

28

Recent regulatory developments in Asia

Singapore

- **Personal Data Protection Act (enacted 2012)**
- **Data Protection Trust Mark (Jan 2019)**
- **DPA proposed a Mandatory Breach Notification Requirement**

The Philippines

- **Data Privacy Act (enacted 2012)**
- **DPO Accountability, Compliance, and Ethics Programme (Dec 2018)**

South Korea

- **One of the strictest data protection law in the world**
- **New Personal Information Protection Act submitted to National Assembly**
- **Adequacy talks with EU ongoing**

29

Recent regulatory developments in Asia

Japan

- **Act on the Protection of Personal Information (amended 2015)**
- **EU-Japan mutual adequacy decisions (adopted Jan 2019)**

India

- **Supreme Court ruled in favour of the right to privacy, as guaranteed under the Constitution (2017)**
- **Draft Personal Data Protection Bill (released Jul 2018)**

NZ

- **New Privacy Bill 2018 before Parliament; to replace the current Privacy Act 1993**

30

Recent regulatory developments in Asia

Thailand

- **Personal Data Protection Act (effective on 28 May 2019)**

Malaysia

- **Personal Data Protection Act 2010**
- **Review of the Act will be conducted (e.g. mandatory data breach notification regime, expansion of the rights of data subjects, etc.)**

Global Data Protection Landscape

As of April
2019

134
countries/regions
with data
protection laws

30+ bills
awaiting
enactment

Source:

<https://gallery.mailchimp.com/1072135a1de8b1660644928a6/files/da8fb6f6-ade4-45c3-9eaf-7f13c8b12316/INT159.pdf>

32

PCPD



HK

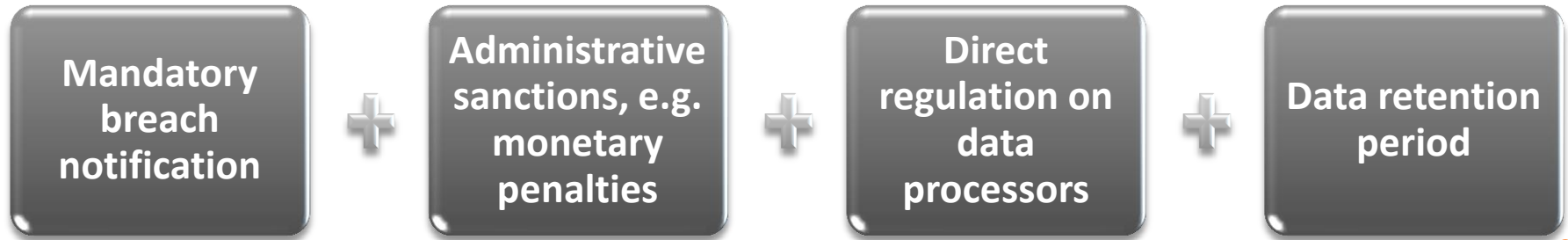


PCPD.org.hk

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

Review of the Hong Kong Personal Data (Privacy) Ordinance

- Last reviewed: 2012
- Balancing the protection of privacy against the free flow of information and other freedoms
- Areas of higher priority:



33

Hong Kong to drive greater regional harmonisation of data protection frameworks

PCPD + Asian Business Law Institute – a project aiming at harmonising the privacy laws in Asia



Phase 1 completed, i.e. understanding the regulations in different Asian jurisdictions



Phase 2 in progress, i.e. drafting Toolbox

Hong Kong and Singapore Signed MOU

31 May 2019

To strengthen cooperation in personal data protection

To engage in the sharing of experiences, exchange of best practices, joint research projects and information exchange involving potential or ongoing data breach investigations

Guide to Data Protection by Design (DPbD) for ICT Systems

https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/Guide_to_DPbD4ICTSystems_May2019.pdf

35

How should companies approach conflicting privacy requirements in different jurisdictions?

- It is possible that the laws in different jurisdictions are conflicting
- Companies should first adhere to the laws of the jurisdictions in which they operate



Cross-border Data Transfer

37

PCPD



HK



PCPD.org.hk

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

Common models (legal bases) for cross-border / boundary data transfer

Examples:

- EU's adequacy decisions

White list

Certifications

Examples:

- APEC CBPRs
- Privacy Shield
- Certification under GDPR

Examples:

- Model contract clauses
- Binding corporate rules

Safeguards

Consent

Necessity

Including necessity for conclusion or performance of contract, etc.

38

Updates on the International Arrangements for Transfer of Personal Data

EU adequacy decisions

- **12 countries obtained adequacy decisions** (*e.g. Canada, New Zealand and Japan*)
- **Discussion in progress with South Korea**
- **Chinese Taipei filed a self-evaluation report to EU in 2018**

APEC CBPRs

- **8 APEC economies joined** (*i.e. Australia, Canada, Chinese Taipei, Japan, Mexico, Singapore, South Korea and the USA*)
- **27 companies certified** (mostly U.S. companies)

EU-US Privacy Shield

- **4,000+ companies certified**
- **European Commission conducted second review** – As required, U.S. has nominated a permanent Ombudsperson to handle complaints on access of personal data by U.S. authorities.

Section 33 of Personal Data Privacy Ordinance (PDPO) [Not yet in force]

- Transfer of personal data outside HK is prohibited **except** under any one of the following specified circumstances:-

1 Transfer to places specified in “White List” [s.33(2)(a)]

2 Adequate data protection regime in the destined jurisdiction [s.33(2)(b)]

3 Written consent by data subjects [s.33(2)(c)]

4 Transfer for avoidance and mitigation of adverse action against data subjects [s.33(2)(d)]

5 Use of personal data is exempted from DPP 3 (use limitation) [s.33(2)(e)]

6 Reasonable precautions and due diligence taken by data users (e.g. contract clauses) [s.33(2)(f)]

Why is s.33 implementation deferred?

Concern from businesses about impact on operations



Concern from businesses about difficulties in compliance, especially SMEs



Businesses demanded guidance from PCPD



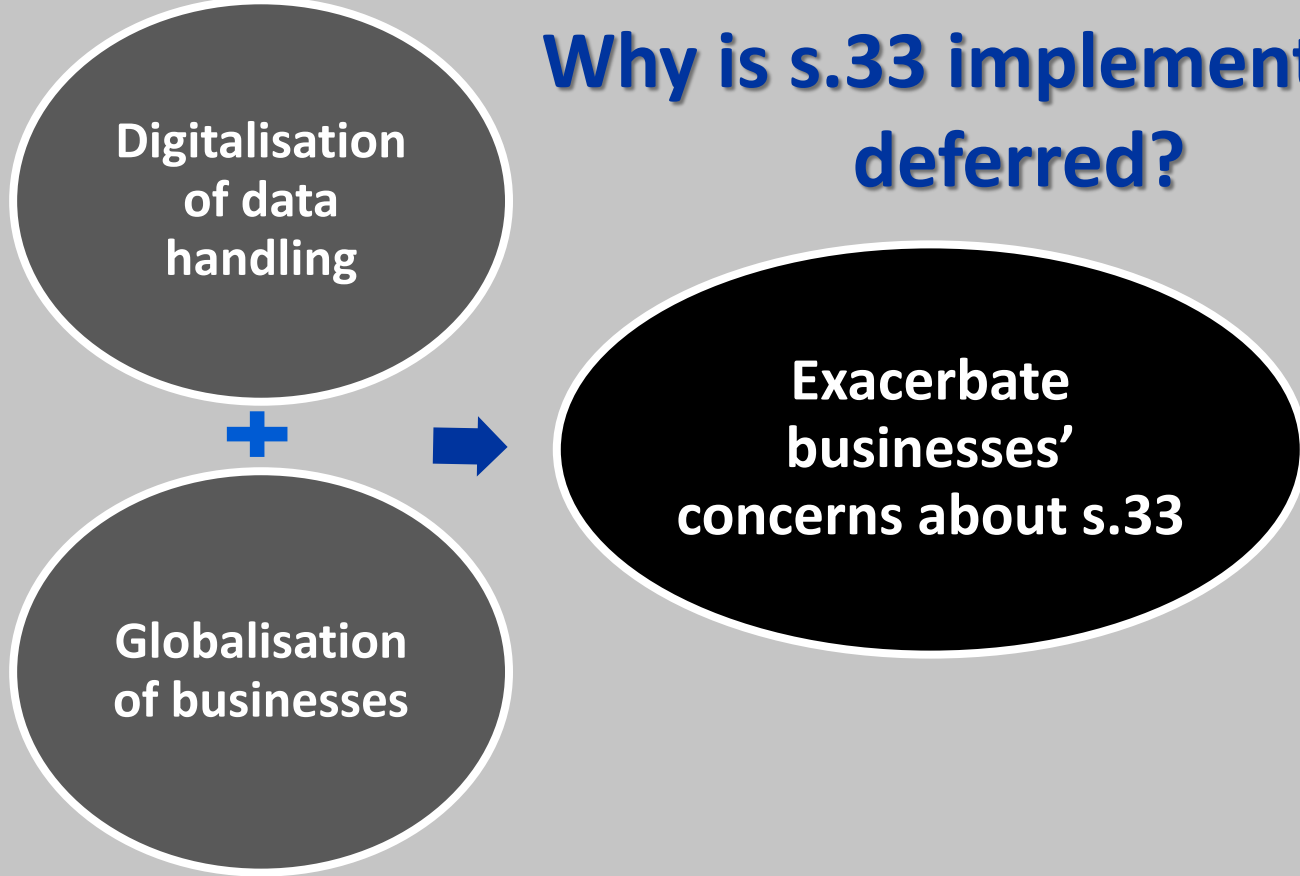
Businesses demanded more time to implement measures to comply

e.g. Impact on international trade and online sales

e.g. Lack of resources and legal knowledge

Guidance Note was issued by the PCPD in December 2014

Why is s.33 implementation deferred?



Existing protection under PDPO without s.33 in operation

DPP 1 requires specification of classes of transferees be given upon collection

DPP 3 prohibits transfer of personal data for **new purposes** without consent

S.65(2) holds data users liable for the **acts of their agents**, including overseas service providers

DPP 2(3) requires data users to prevent their processors from **retaining** personal data longer than necessary

DPP 4(2) requires data users to ensure **security** of personal data transferred to their processors

Existing protection under PDPO without s.33 in operation

Even if s.33 is not in force, for data transferred from other jurisdictions to Hong Kong, parties can impose ***contractual restrictions on onward transfer*** to places outside Hong Kong.

(See also other Model Clauses attached)

Recent work by PCPD and HKSAR Government on s.33

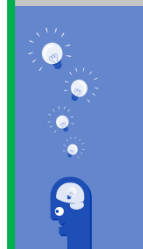
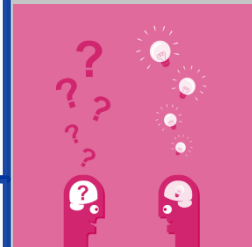
2014 -
2015

To address businesses' demand for guidance, PCPD issued **Guidance Note** on compliance with requirements of s.33, with a set of **model contract clauses** recommended

More concerns raised by businesses in response to the **Guidance Note**

e.g.-

- Unclear about the definition of “**personal data**” and “**transfer**”
- Difficult for SMEs to impose **contract clauses** to services providers?
- What if a “White Listed” region is subsequently **delisted**?
- **Lack of resources** to monitor service providers abroad
- **Lack of information** about the location of cloud servers



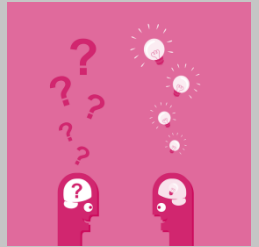
45

Recent work by PCPD and HKSAR Government on s.33

2015-
2016

Government commissioned a consultant to conduct a **Business Impact Assessment (BIA) Study** on implementation of s.33

PCPD rendered comments to the consultant on the interpretation, application and compliance issues of s.33



46

PCPD



HK



PCPD.org.hk

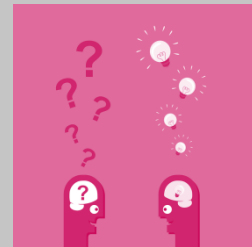
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Recent work by PCPD and HKSAR Government on s.33

2018

Seven issues of concerns raised by Government's consultant in the BIA Study which require further studies

PCPD engaged a **consultant** to explore how restriction on cross-border data transfer may be implemented in light of these **seven issues of concerns**



47

PCPD



HK



PCPD.org.hk

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

The seven issues of concerns

1. How "transfer" under s.33 and "personal data" are to be defined

2. The mechanism for reviewing and updating the "white list" under s.33

3. Whether the adoption of existing rules and standards in highly regulated industries (e.g., financial industry) would allow a data user to be regarded as having met the requirements of s.33

48

The seven issues of concerns

4. The ancillary measures or alternatives to facilitate the implementation of s.33

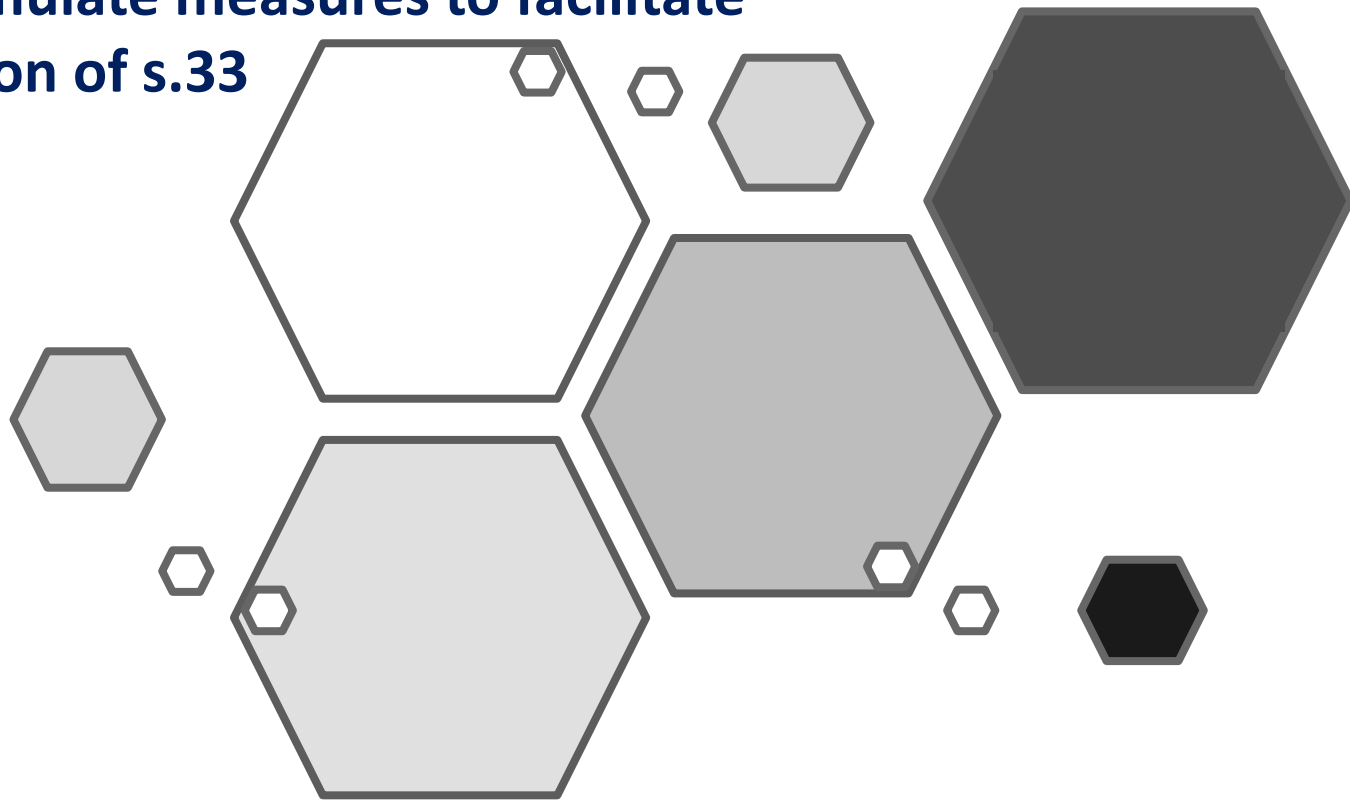
5. Enforcement issues of s.33 and means to tackle them

6. The criteria or yardsticks for deciding whether a data user has "*taken all reasonable precautions and exercised all due diligence*" under s.33

7. Suggestions on the forms of support or guidance from the PCPD to help businesses understand and comply with the requirements of s.33

49

PCPD will formulate measures to facilitate implementation of s.33



Model Contract Clauses Recommended by PCPD

See: PCPD's "*Guidance on Personal Data Protection in Cross-border Data Transfer*"

1. Obligations of the Transferor

2. Obligations of the Transferee

3. Liability and indemnity

4. Settlement of disputes

5. Termination

6. Third Party Rights

A stylized graphic of a human head profile in silhouette, filled with a glowing blue and yellow network of nodes and lines, representing artificial intelligence or neural networks. The background is a dark blue gradient with faint circular patterns.

Artificial Intelligence

52

PCPD



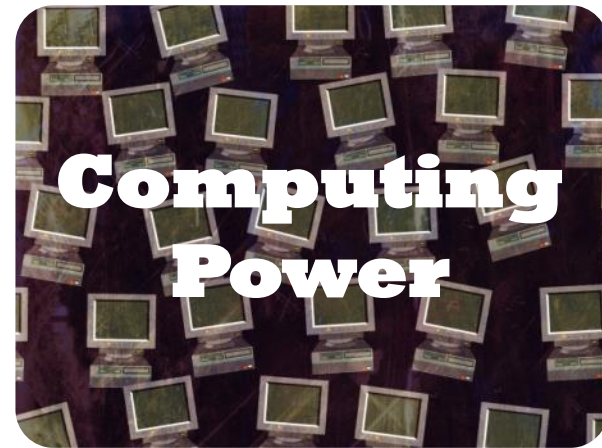
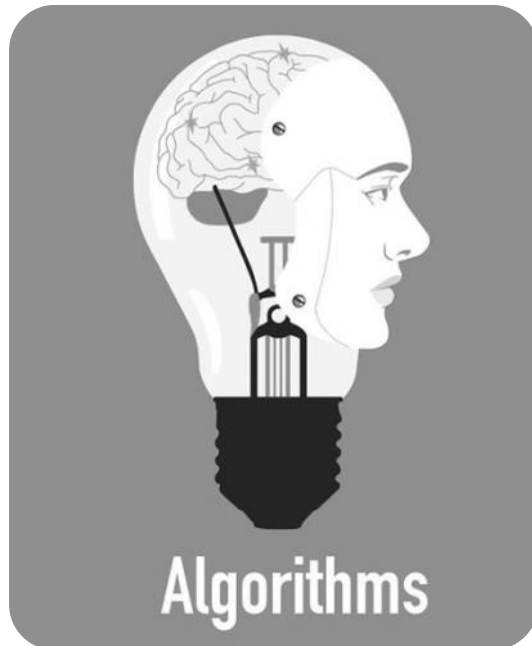
HK



[PCPD.org.hk](https://www.pcpd.org.hk)

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

AI elements



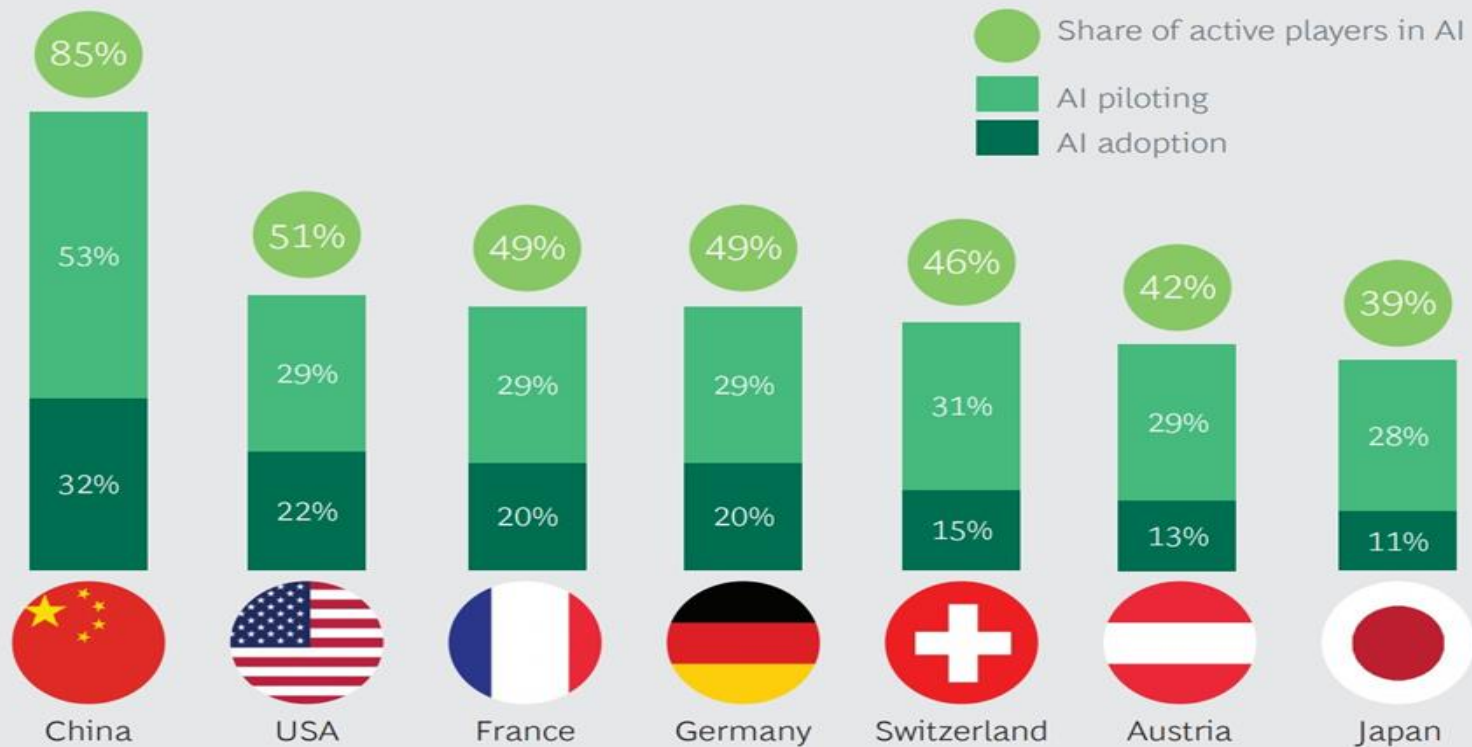


Mainland China

1.4 Billion population

- 1.3 billion 3G /4G mobile accounts
- 71 billion gigabytes mobile traffic in 2018

Share of active players in AI by country



Source: Boston Consulting Group (Dec 2018)

World's biggest AI unicorn, SenseTime was founded in HK

Hong Kong

HK Ranked 2nd in the APAC AI Readiness Index*

*Source: Asia Pacific AI Readiness Index by Salesforce (Apr 2019). Jurisdiction covered in the index are Australia, Hong Kong, India, Indonesia, Malaysia, Philippines, Singapore and Thailand

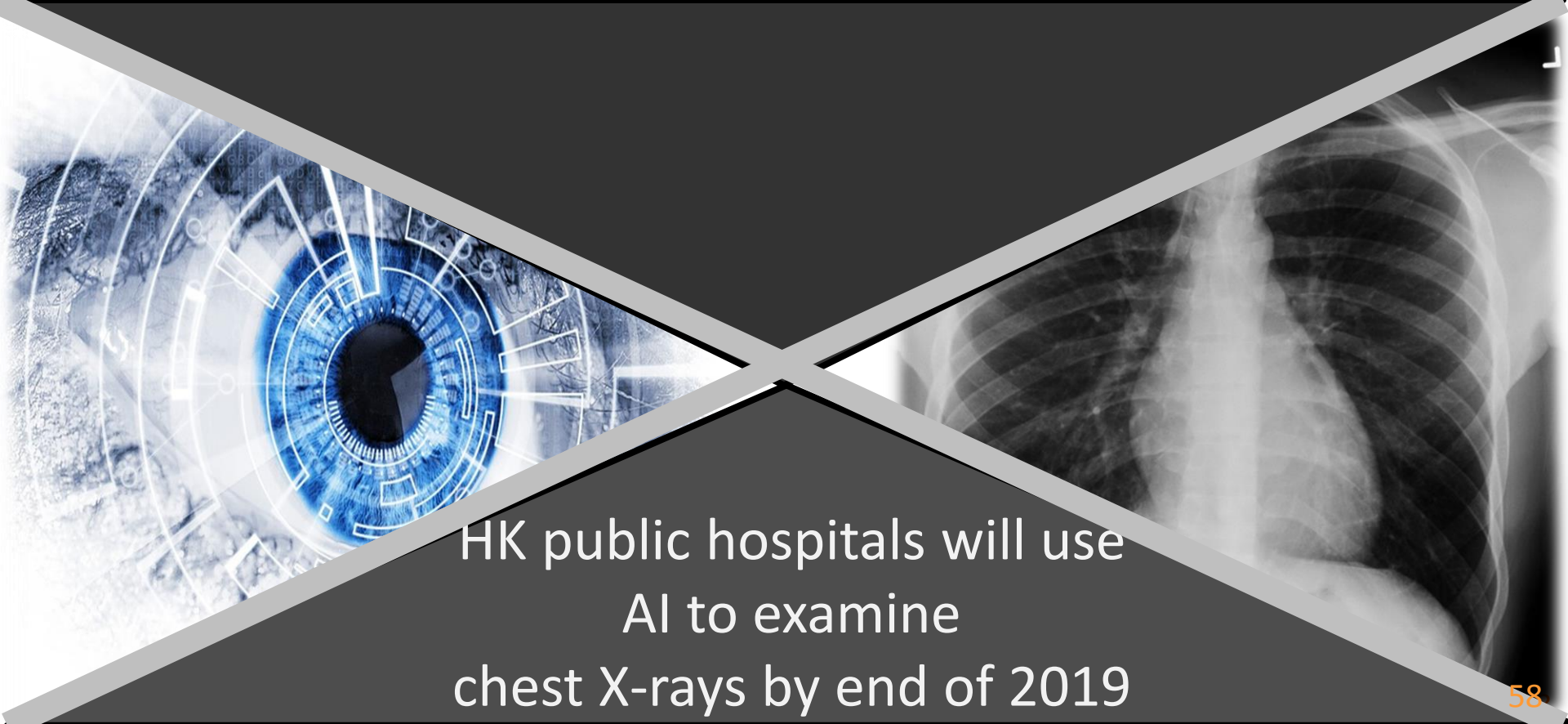
AI robot “Sophia” developed by a HK company



- runs on a cloud-based AI


- simulates human facial expression

- first robot in the world recognised with a citizenship (Saudi Arabia, 2017)



HK public hospitals will use
AI to examine
chest X-rays by end of 2019

58

- 
- First Big Data Arbitration Center Established in Shenzhen, China in 2017
 - Use of AI for pre-arbitration assessment and writing of decisions

San Francisco

Use of Facial Recognition
Software by Police and other
Government Agencies Ban

60

Illinois

Artificial Intelligence Video Interview Act

- ❖ Notification
- ❖ Explanation
- ❖ Obtain Consent



61

Efficiency

Effectiveness



AI

Bias

Unfair discrimination

Inequality

62

PCPD



HK

PCPD.org.hk

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

Microsoft – IDC Study: Artificial Intelligence adoption to increase rate of innovation and employee productivity gains by more than double by 2021

May 8, 2019 | Doris Hui



- Artificial Intelligence (AI) will more than double the rate of innovation and employee productivity gains in Hong Kong by 2021.

Microsoft – IDC Study: Only 31% of consumers in Asia Pacific trust organizations offering digital services to protect their personal data

April 16, 2019 | Microsoft Asia News Center



- Nearly 40% of consumers in the region have had their trust compromised when using digital services;
- Only 5% of consumers prefer to transact with an organization that offers a cheaper but less trusted digital platform;
- Consumers have the highest expectations of trust from financial services, healthcare and education sectors;

Source: Microsoft (April & May 2019)

63

PCPD



H K



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

Data Ethics

2017

Ethics on AI -

1st being discussed at the ICDPPC meeting held in Hong Kong

2018

“Ethical Accountability Framework for Hong Kong, China” published by PCPD

“Declaration on Ethics and Data Protection in Artificial Intelligence” made by the ICDPPC in Brussels

ICDPPC Permanent Working Group on Ethics and Data Protection in AI established (co-chaired by CNIL, EDPS and PCPD (HK))

2019

“Ethics Guidelines for Trustworthy AI”

issued by the European Commission

Ethics on AI first discussed in Hong Kong (2017)

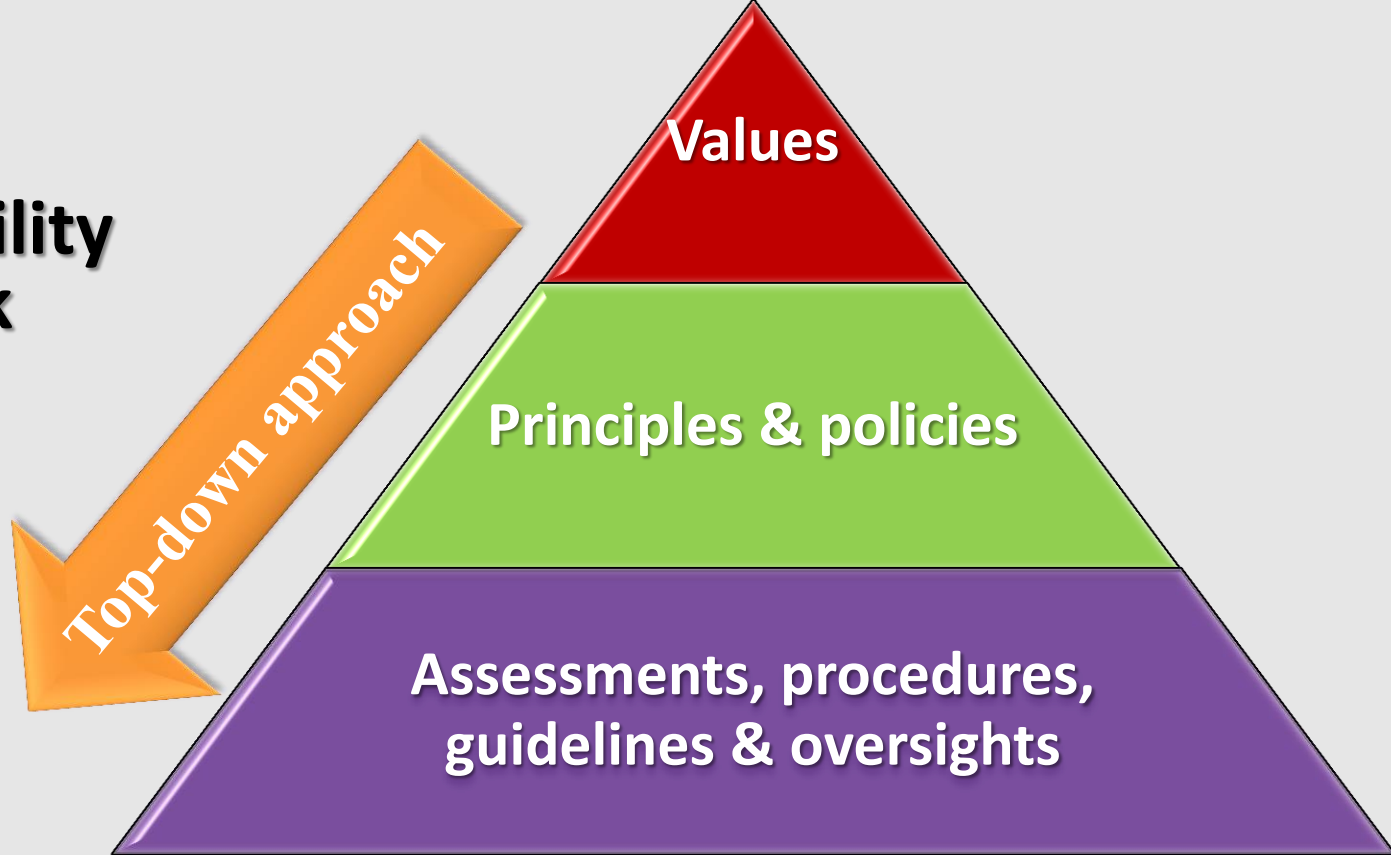


*“Data users need to add value beyond just complying with the regulations. Discussions about **“New Digital Ethics”**, the relevant ethical standard and stewardship have already begun. Surely the deliberations will go on. In the not far away future, we may come up with an **“Equitable Privacy Right”** for all stakeholders.”*

Stephen Kai-yi Wong
Opening speech at 39th ICDPPC (2017)

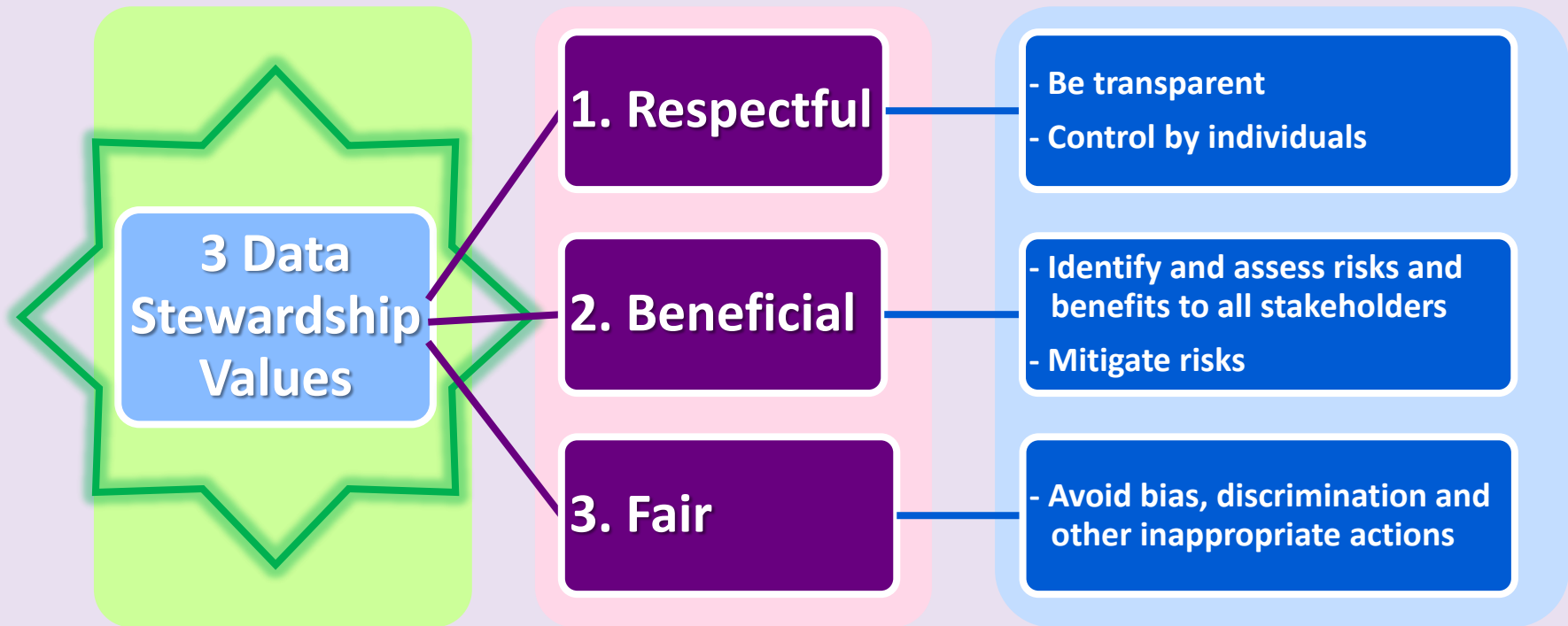
65

PCPD's Ethical Accountability Framework (2018)

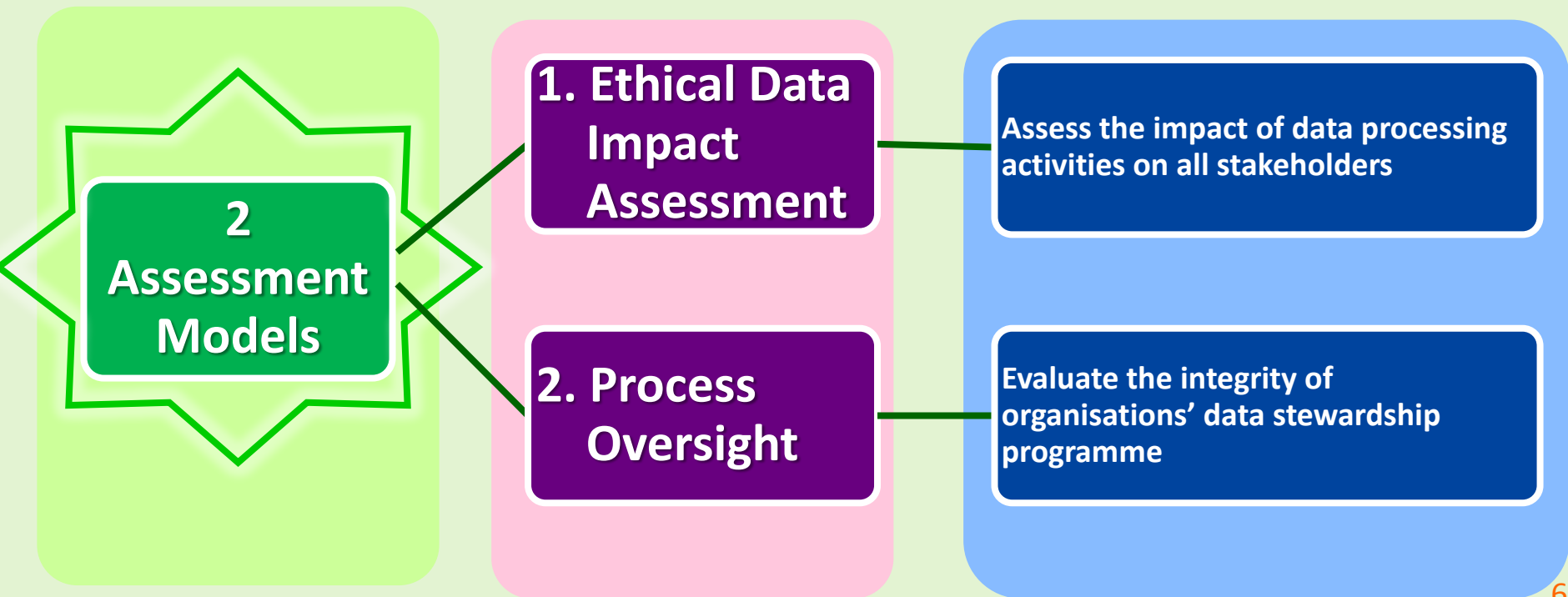


66

Multi-stakeholders Approach – Three Core Values



Multi-stakeholders Approach – Two Assessment Models



68

Data Ethics - Implementation

Privacy
by
Design



Ethics
by
Design

Step 1: Analyse the business objective and purpose of the data processing activity

Step 2: Assess the nature, source, accuracy and governance of the data

Step 3: Conduct impact assessment, i.e. risks and benefits to the individuals, the society and the organisation itself

Step 4: Balance between expected benefits and the mitigated risks to all stakeholders

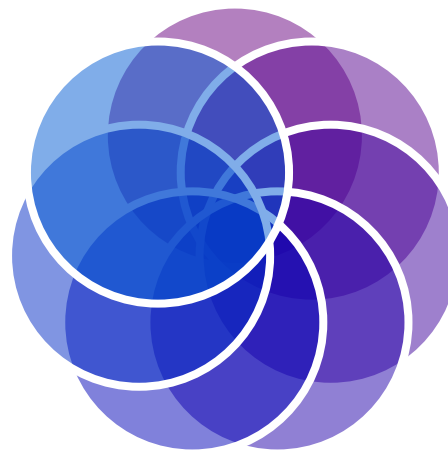
ICDPPC Declaration on Ethics and Data Protection in Artificial Intelligence (2018): Six Core Principles



Reducing
biases or
discriminations

Empowerment
of every
individual

Fairness
principle



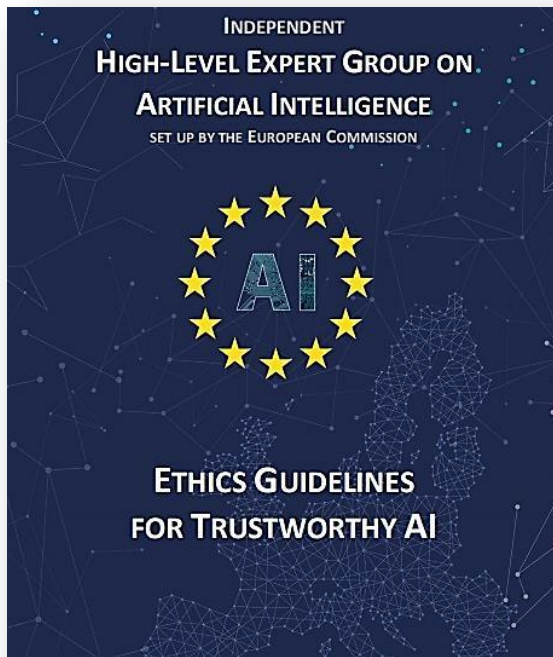
Continued
attention
and vigilance

Systems
transparency
and
intelligibility

Ethics by design

70

EU's "Ethics Guidelines for Trustworthy AI" (2019)



7 key requirements:

1. **Human agency and oversight**
2. **Technical robustness and safety**
3. **Privacy and data governance**
4. **Transparency**
5. **Diversity, non-discrimination and fairness**
6. **Societal and environmental well-being**
7. **Accountability**

71

PCPD



H K

PCPD.org.hk

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



PCPD information leaflet

Data Ethics for Small and Medium Enterprises





HKMA's circular on 3 May 2019

- To all authorized institutions
- Encourages them to adopt and implement the Ethical Accountability Framework in the development of fintech products and services

<https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190503e1.pdf>

Data ethics in mainland China

Expert committee on AI governance set up by the Ministry of Science and Technology in February 2019

Minister of Science and Technology of China, WANG Zhigang: (May 2019)

- *Drafting of the AI governance guidelines is progressing well. The draft guidelines will be released soon.*

74

A symposium on AI ethics and Internet governance, Beijing, May 2019

Co-founder of SenseTime, XU Li:
(May 2019)

- *New rules on facial recognition are crucial towards the wider adoption of this form of AI technology around the world.*

Core values of personal data protection

- Personal data privacy right is a fundamental human right
- Human right is about the dignity of a human being
- A proper balance should be struck between personal data privacy right and other human rights where conflicts occur
- Personal data privacy right should not stifle ICT and economic developments

Regulating for Results

Enforcer

Educator

Facilitator

77

PCPD



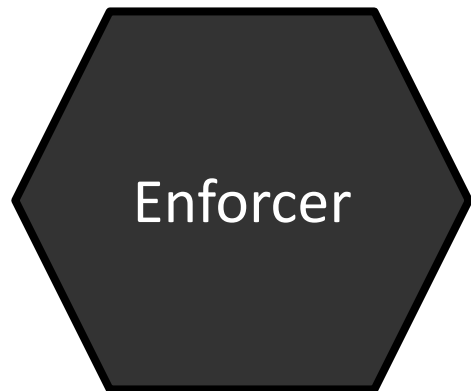
HK



PCPD.org.hk

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

Fair enforcement, taking into account



- Statutory requirements
- Privacy expectation
- Legitimate interest

Children PRIVACY

A one-stop portal for children to learn and understand personal data privacy, and for teachers and parents to help those under their care in how to protect their personal data.

Protect, Respect Personal Data



Educator

Student Ambassador Programme

學生大使活動

2018



保障私隱學生大使暨「學校夥伴邀請計劃」計劃2018



79

PCPD



HK



PCPD.org.hk

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

Education campaigns in 2018

- 18 promotional and education programmes with 262,145 participants
- 106 schools joined “Student Ambassador for Privacy Programme”
- 421 professional workshops, talks and seminars

80

PCPD

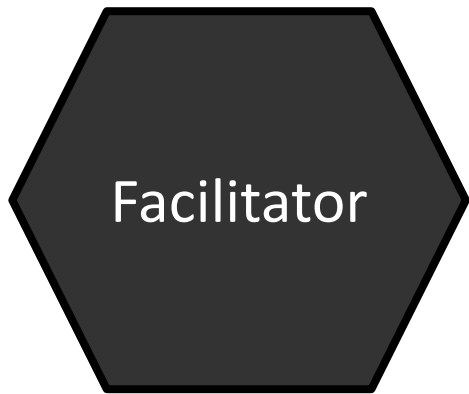


HK

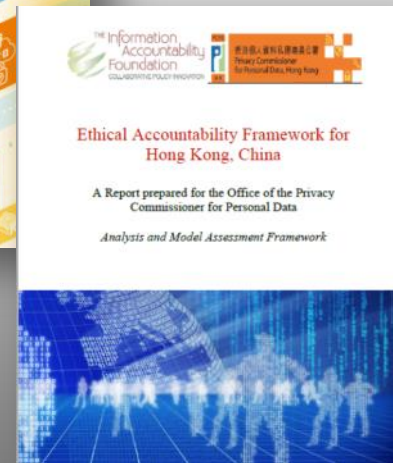


PCPD.org.hk

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



Lawful, accountable
and ethical use of
personal data



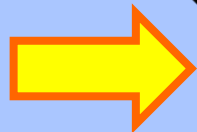
PCPD's Roles – Enforcer + Educator + Facilitator

PCPD's Strategic Focus

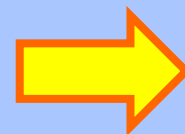
Fair Enforcement



Engaging

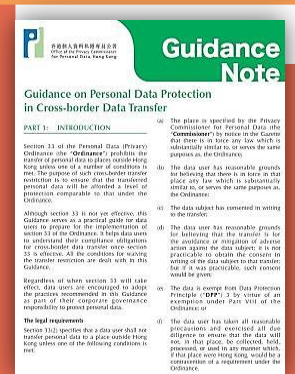
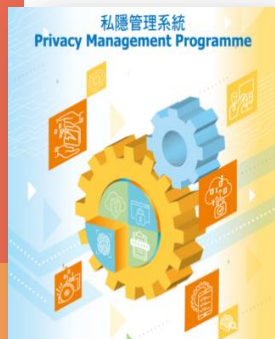
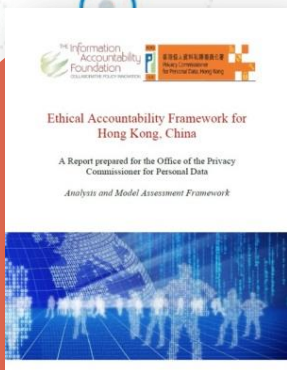


Incentivising



Privacy-friendly Culture

Download our publications:



Contact Us



Copyright



This PowerPoint is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this PowerPoint, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.

- ☐ Hotline 2827 2827
- ☐ Fax 2877 7026
- ☐ Website www.pcpd.org.hk
- ☐ E-mail enquiry@pcpd.org.hk
- ☐ Address 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, HK