The Australian Chamber of Commerce in Hong Kong

11 September 2019 | Hong Kong

A Unique and Irreplaceable Attribute of Hong Kong SAR: Free Flow of Information and Personal Data Protection Regime

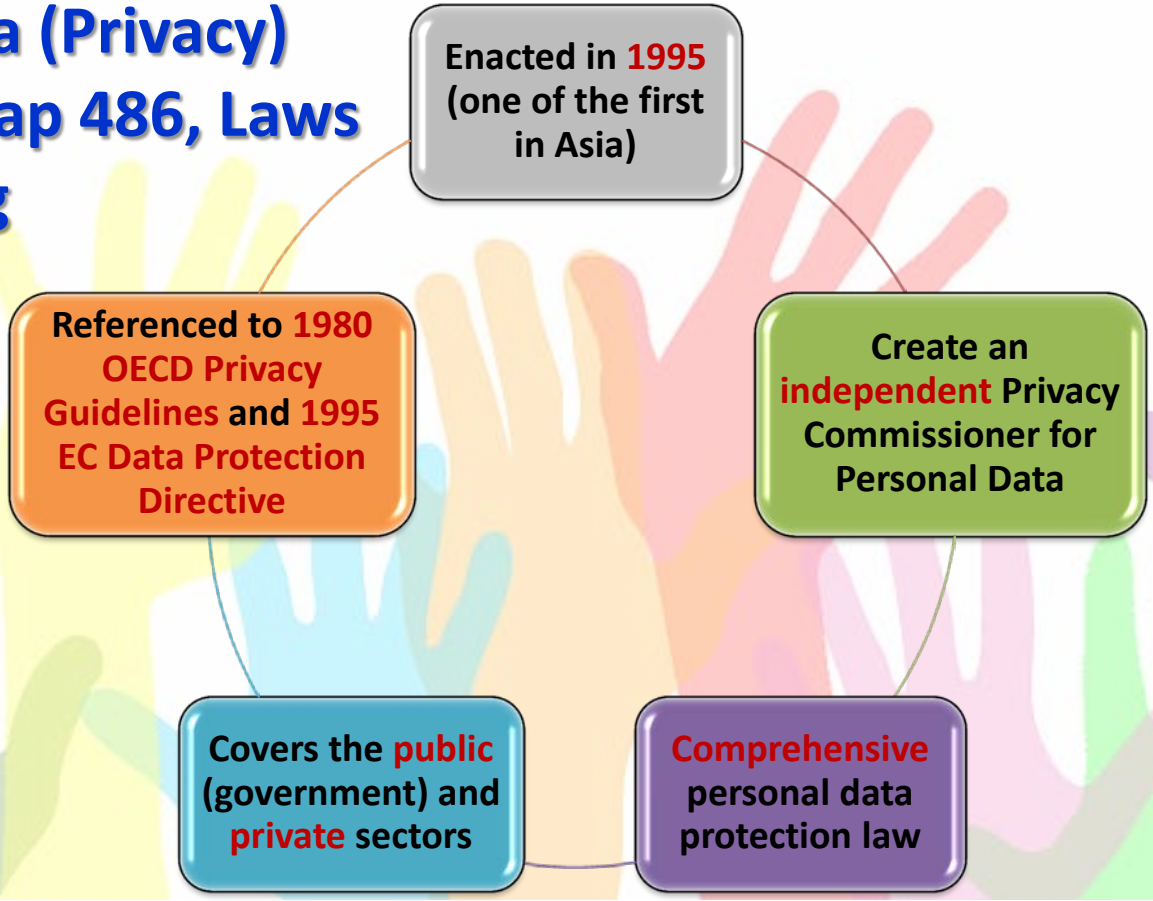
Stephen Kai-yi Wong, Barrister

Privacy Commissioner for Personal Data, Hong Kong, China

Personal Data Privacy

Fundamental Human Right

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



International Covenant on Civil and Political Rights

Extended to HK in 1976

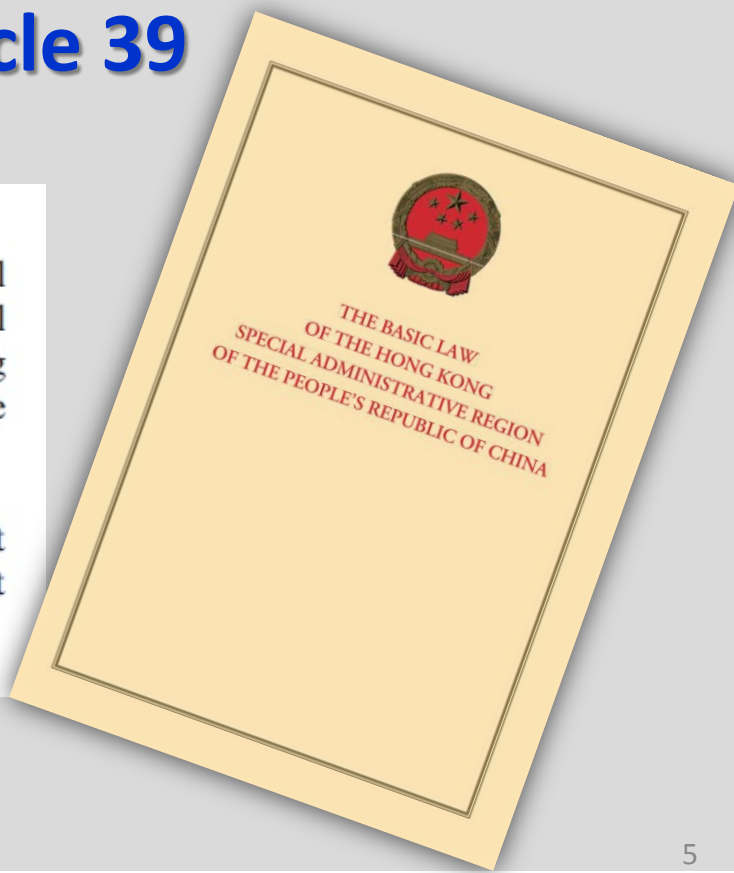
"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." **[Art. 17 of the ICCPR]**

The Basic Law, Article 39

Article 39

The provisions of the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and international labour conventions as applied to Hong Kong shall remain in force and shall be implemented through the laws of the Hong Kong Special Administrative Region.

The rights and freedoms enjoyed by Hong Kong residents shall not be restricted unless as prescribed by law. Such restrictions shall not contravene the provisions of the preceding paragraph of this Article.



The Basic Law – Examples of Human Rights Protection

Guarantee freedom of speech, of the press and of publication, etc. [Art. 27]

Prohibit arbitrary or unlawful search of, or intrusion into, a resident's home or other premises [Art. 29]

Guarantee freedom and privacy of communication [Art. 30]

Provisions of the International Covenant on Civil and Political Rights, etc. remain in force and shall be implemented through the law of HKSAR [Art. 39]

Hong Kong Bill of Rights Ordinance

Article 14

Protection of privacy, family, home, correspondence, honour and reputation

(1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

Hong Kong's Unique & Irreplaceable Attributes

"Hong Kong…has many unique attributes…for instance, free and open economy, efficient business environment, advanced professional services sector, well-established infrastructure and facilities, internationally recognised legal system, free flow of information and large supply of quality professionals…"

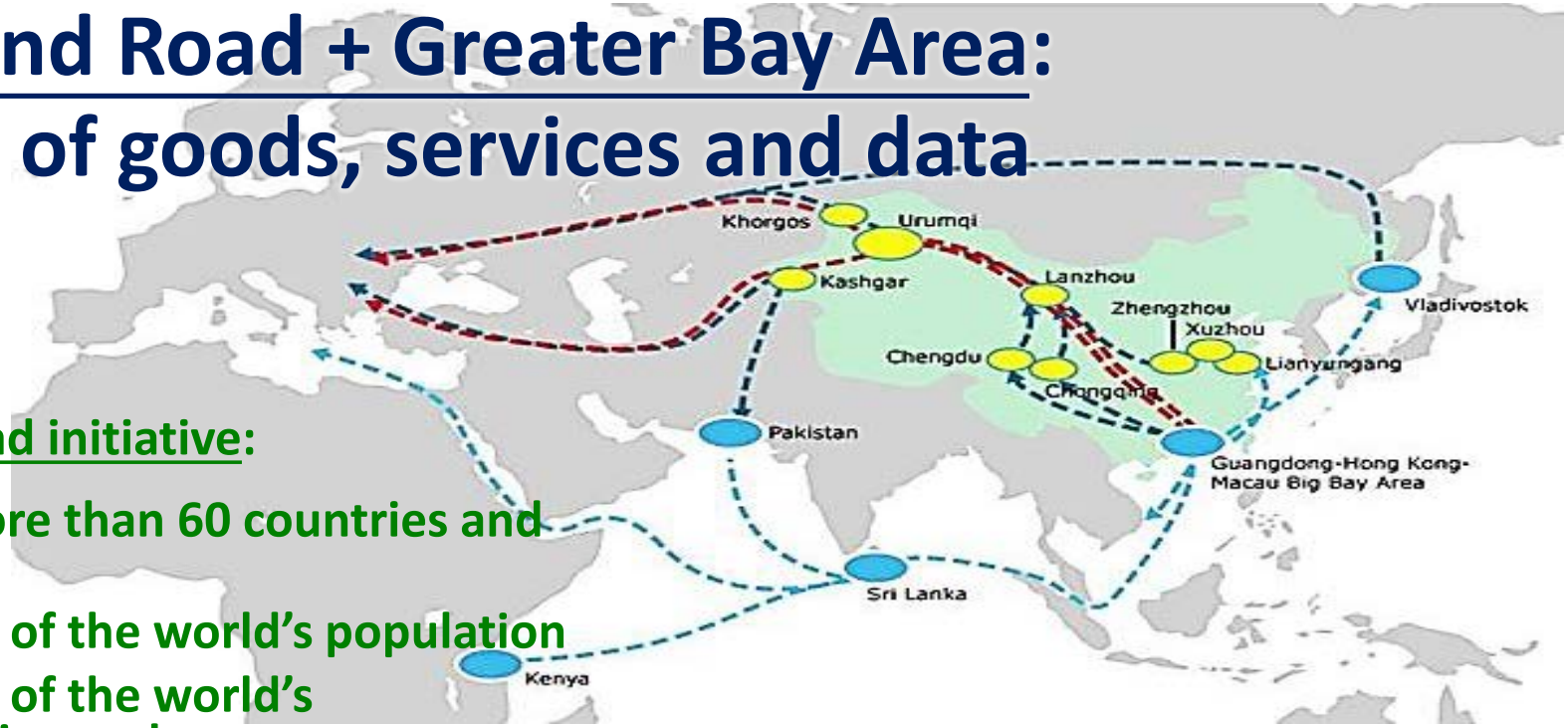
Mr ZHANG Dejiang,
Chairman of the Standing Committee of the National People's Congress of the PRC
Keynote Speech,
Belt and Road Summit, 18 May 2016

Hong Kong's Unique & Irreplaceable Attributes

"In the country's reform and opening in the new era, Hong Kong and Macao still possess special, unique and irreplaceable attributes. "

Xi Jinping, President of China
Speech at the meeting with Hong Kong delegation in the Celebration of the 40th Anniversary of the Reform and Opening Up of the Country
12 November 2018

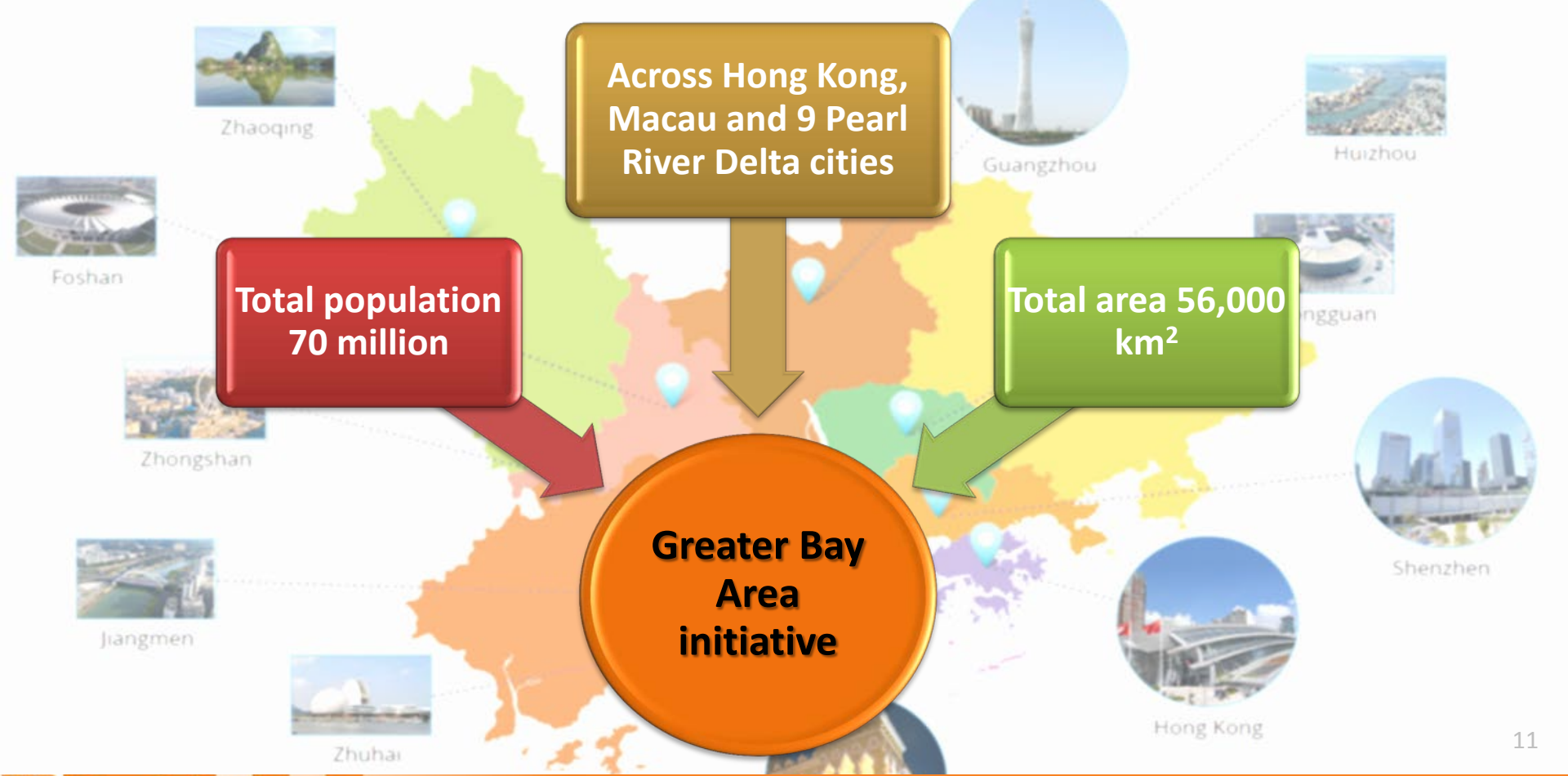
Belt and Road + Greater Bay Area: Flows of goods, services and data



Belt and Road initiative:

- Covers more than 60 countries and regions
- Over 62 % of the world's population
- Over 34 % of the world's merchandise trade
- Around 31 % the world's GDP

Source: Hong Kong Trade Development Council


Across Hong Kong, Macau and 9 Pearl River Delta cities
Total population 70 million
Total area 56,000 km²
Greater Bay Area initiative
Zhaoqing
Guangzhou
Huizhou
Foshan
Zhongshan
Shenzhen
Jiangmen
Zhuhai
Hong Kong

Hong Kong's Unique Advantages as Regional Data Hub for Belt & Road and Greater Big Area Initiatives

Sound and well-developed legal system

'One Country, Two Systems'

Highly stable power supply (reliability > 99.999%)#

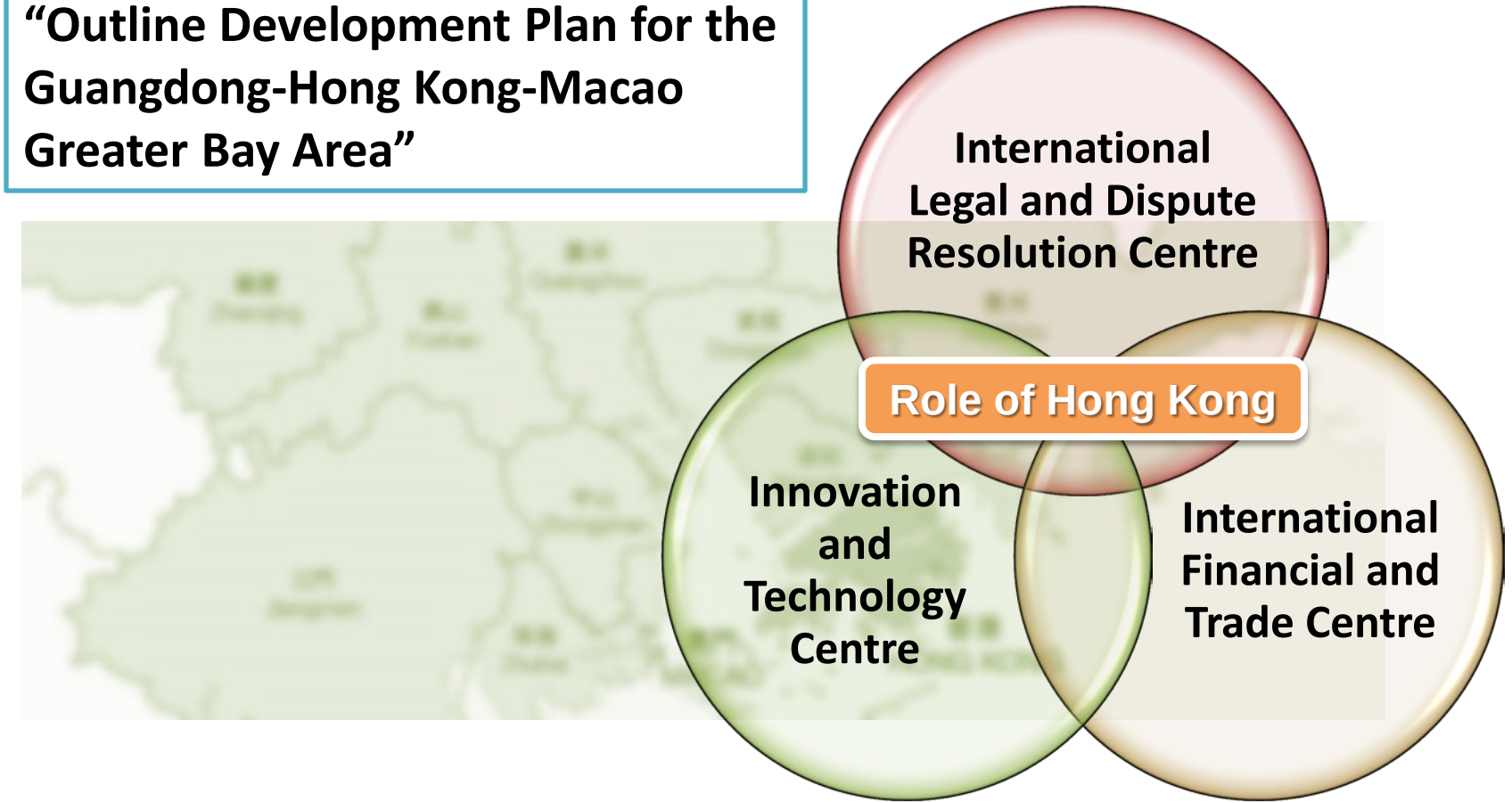
Free flow of information

Ranked no. 2 in Asia in Cloud Readiness Index 2018*

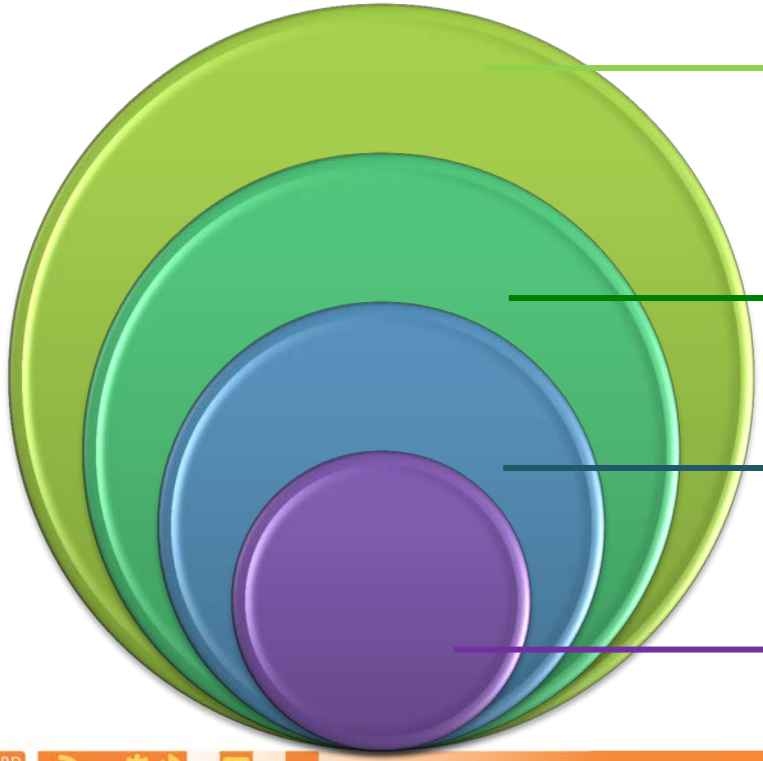
"Super connector" between mainland China and the rest of the world

Sources:
 # CLP Power & HK Electric
***Asia Cloud Computing Association: Cloud Readiness Index 2018**

“Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area”



“Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area”



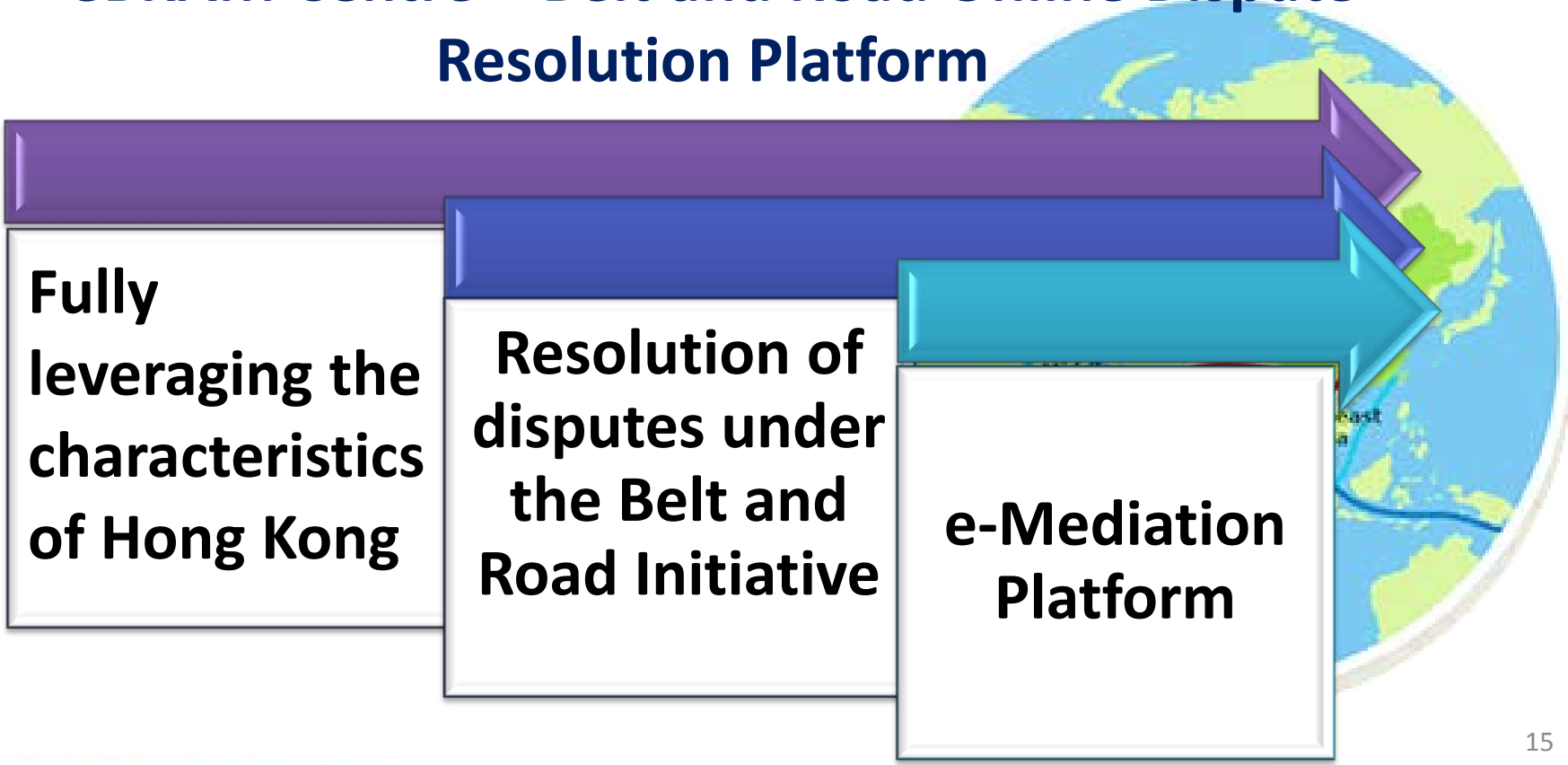
Exploration of establishment of common standards, open data ports and development of connected public application platforms

Development of plans to strengthen the mangement of cross-border use of medical data and biological samples

Joint development of a Greater Bay Area big data centre

Facilitation of cross-border and regional mobility of people, goods, capital and information

eBRAM Centre – Belt and Road Online Dispute Resolution Platform



Hong Kong's Role as regional data centre

No border personal data flow

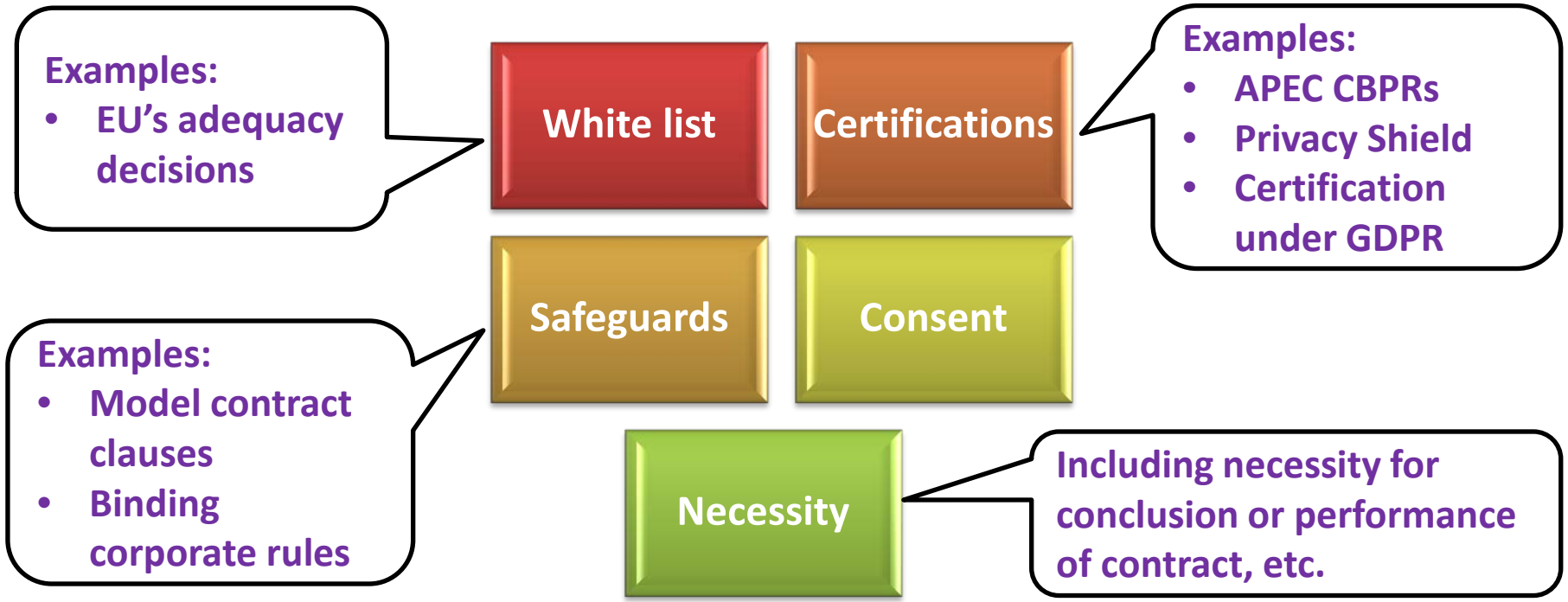
+

Facilitation of technology development （e.g. AI, Big Data, etc.）

→

Enhance the importance of data protection

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



Updates on the International Arrangements for Transfer of Personal Data

EU adequacy decisions	• **13 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)* • **20+ group of 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 → **e.g. Impact on international trade and online sales**

+

Concern from businesses about difficulties in compliance, especially SMEs → **e.g. Lack of resources and legal knowledge**

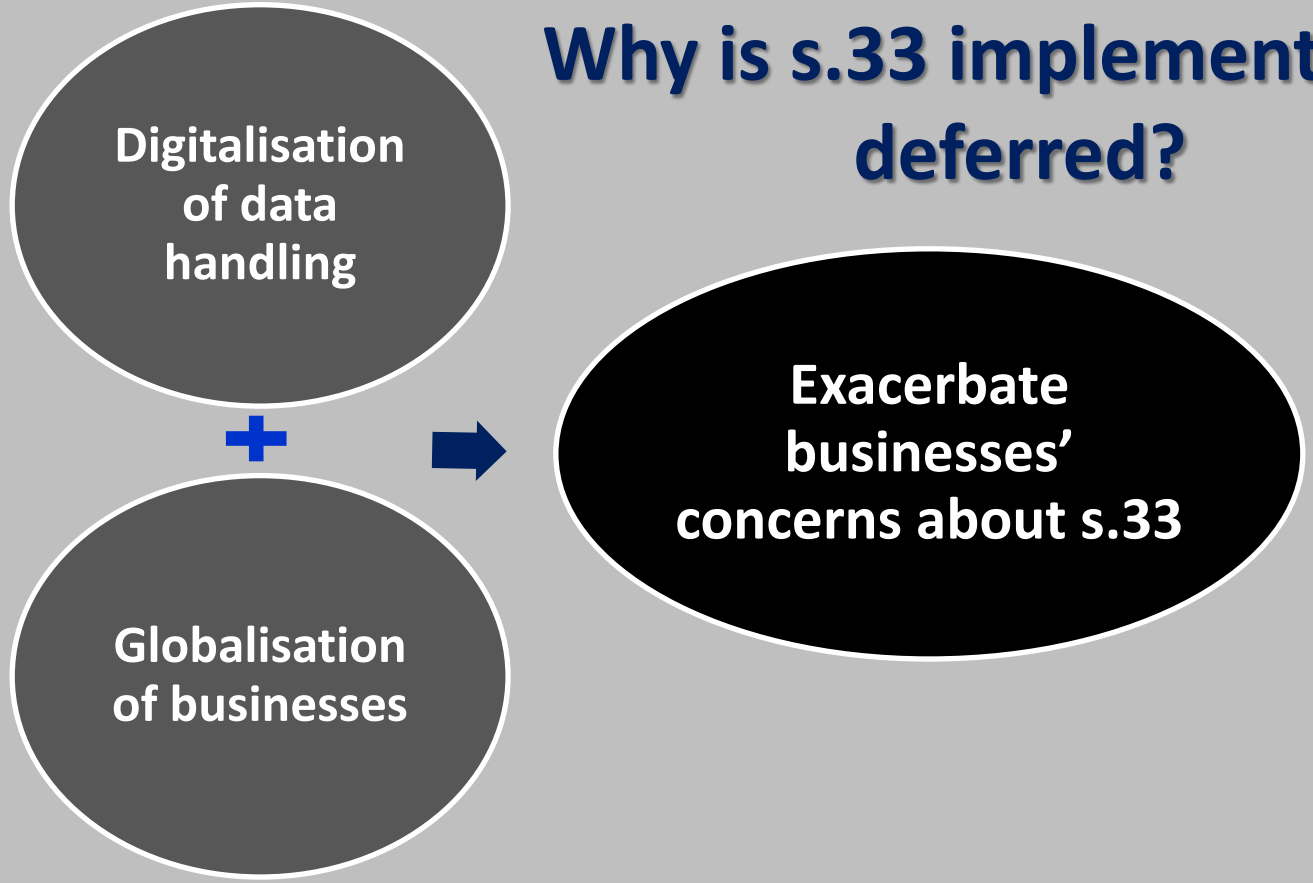
+

Businesses demanded guidance from PCPD → **Guidance Note was issued by the PCPD in December 2014**

+

Businesses demanded more time to implement measures to comply

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

Contractual restrictions on onward transfer to places outside Hong Kong

See Recommended Model Clauses in PCPD's "Guidance on Personal Data Protection in Cross-border Data Transfer"
https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_crossborder_e.pdf

Recent work by PCPD and HKSAR Government on s.33

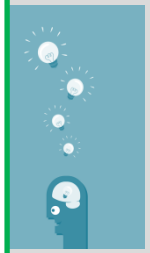
2014 - 2015

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



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

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

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

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

Possible future steps

Providing simplified model contract clauses targeted at SMEs

Differentiating the obligations of the transferee under the model contract clauses (i.e. separate set of clauses for "*data user to data user transfers*" and "*data user to data processor transfers*"

Inserting additional exceptions allowing cross-border / boundary data transfer, e.g. certification schemes

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**


Data Breach

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.

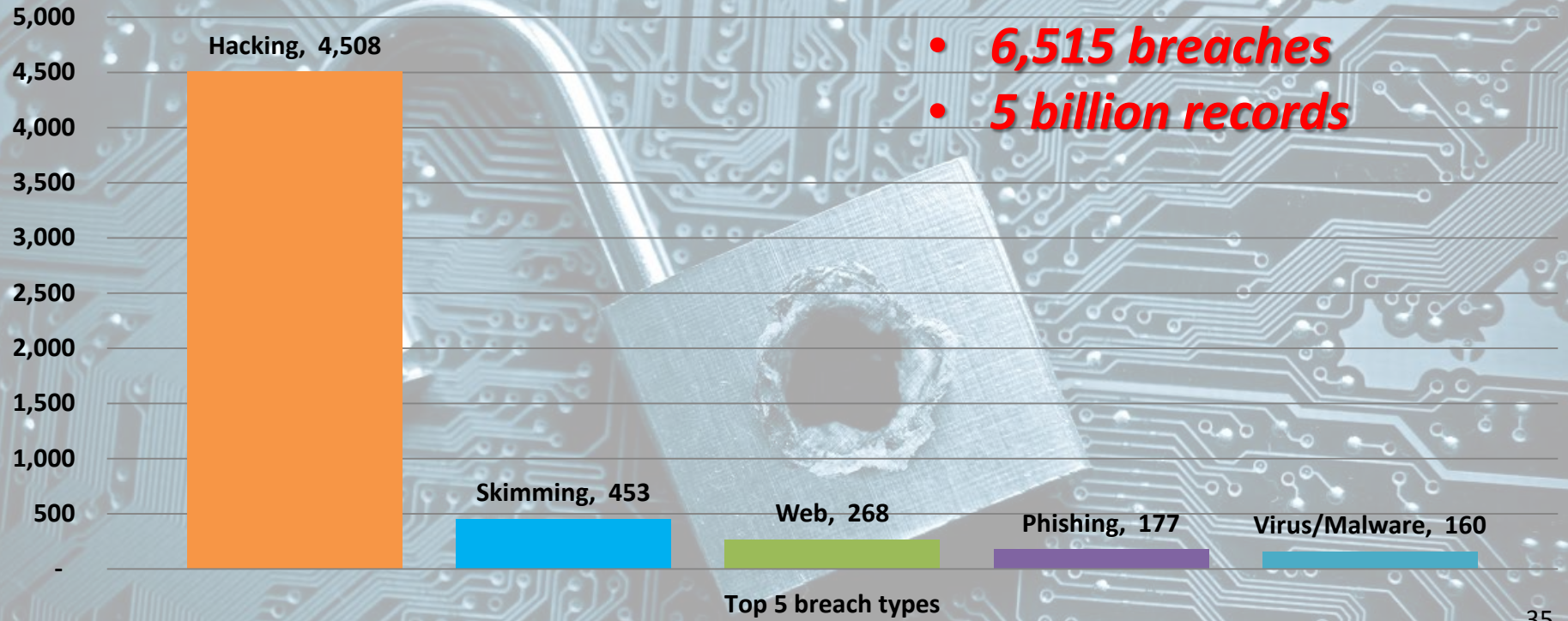
Shift of Regulatory Emphasis

Data collection/ use

Data security

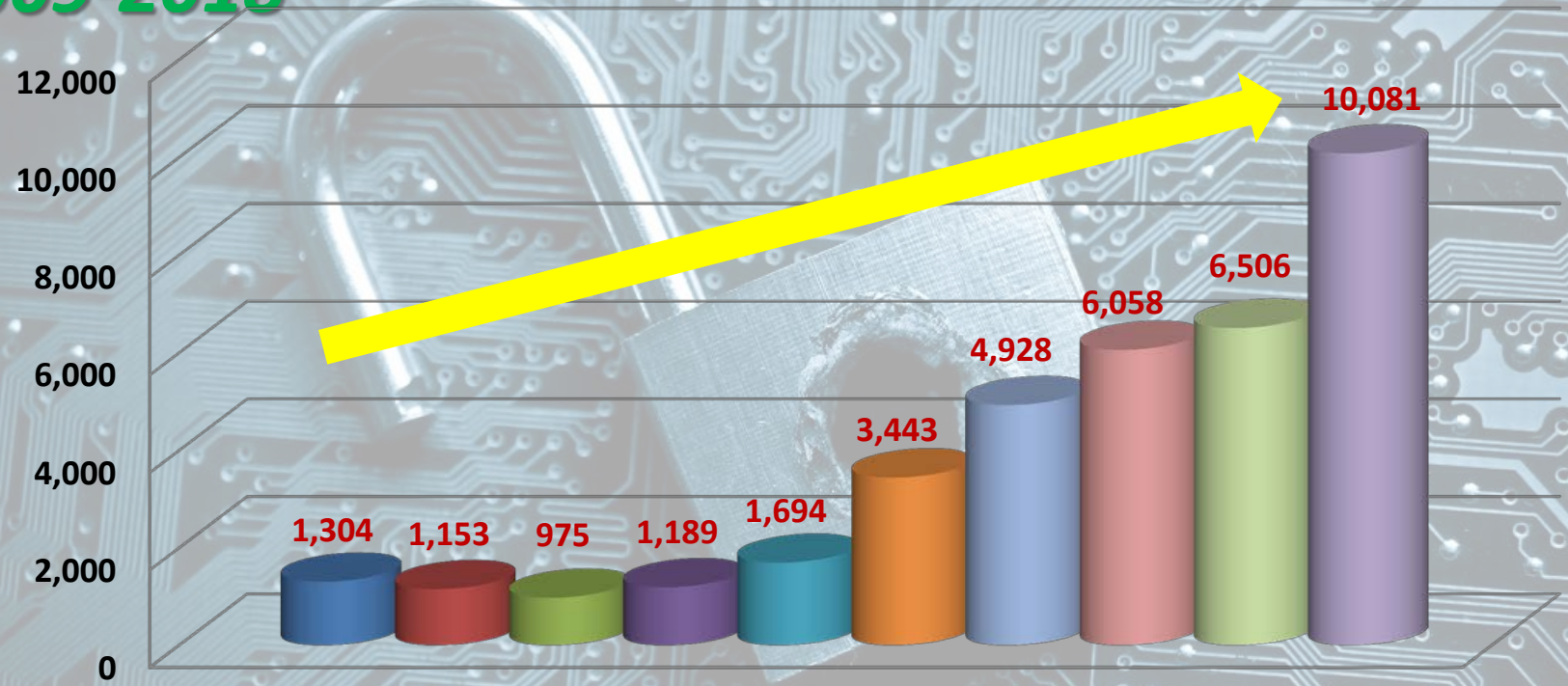
Data Breach Incidents

Publicised data breach 2018 (global)

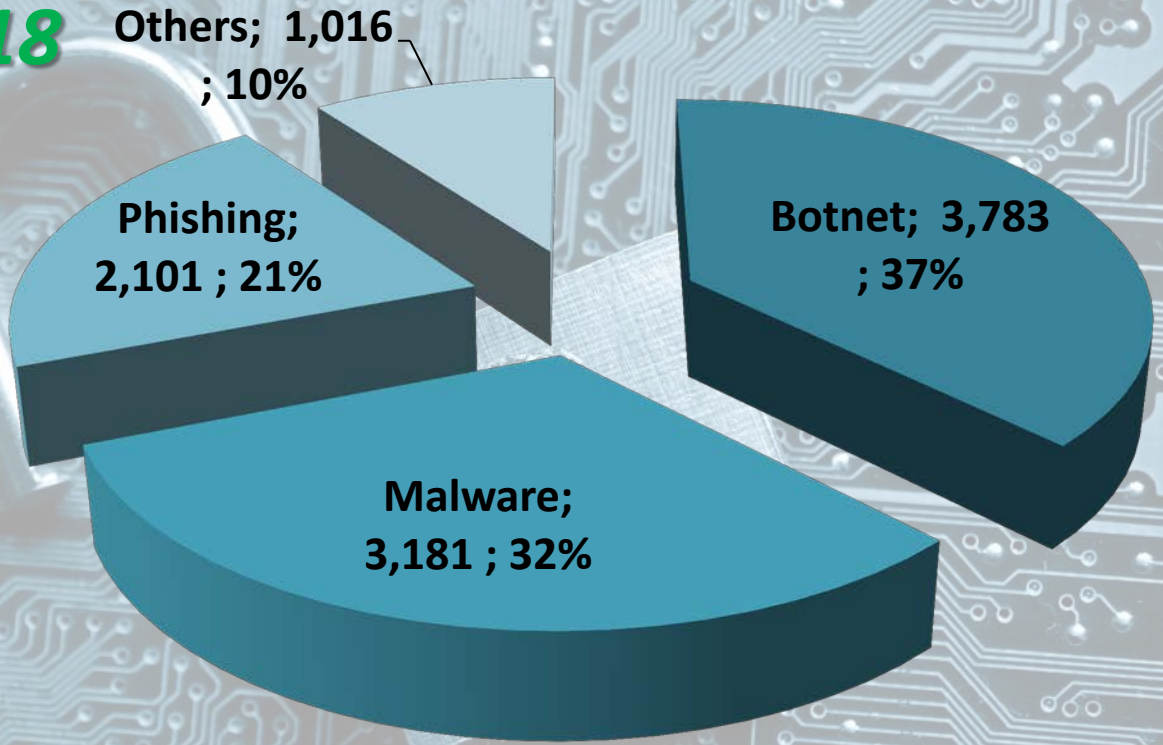


- 6,515 breaches
- 5 billion records

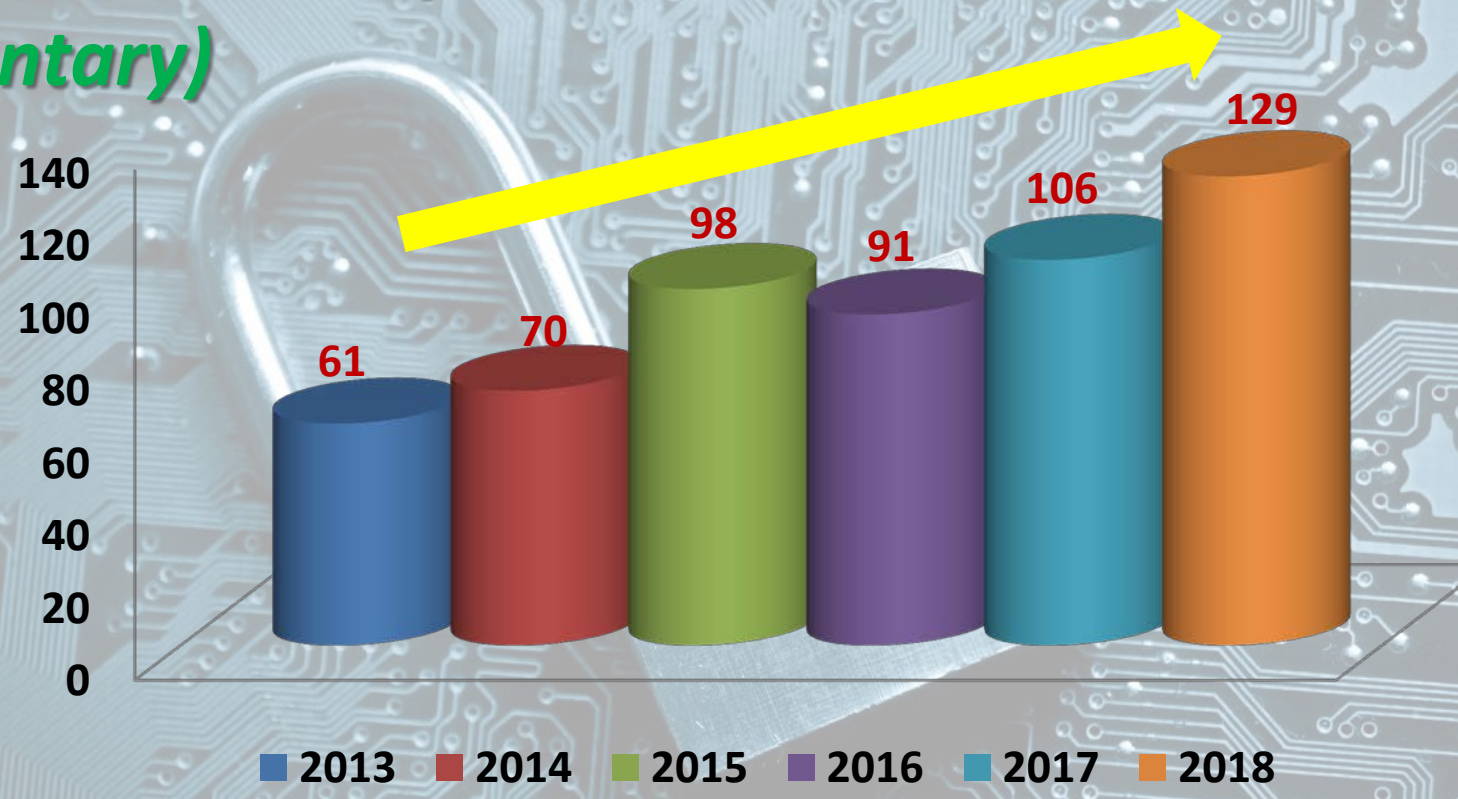
Cybersecurity incidents reported to HKCERT 2009-2018



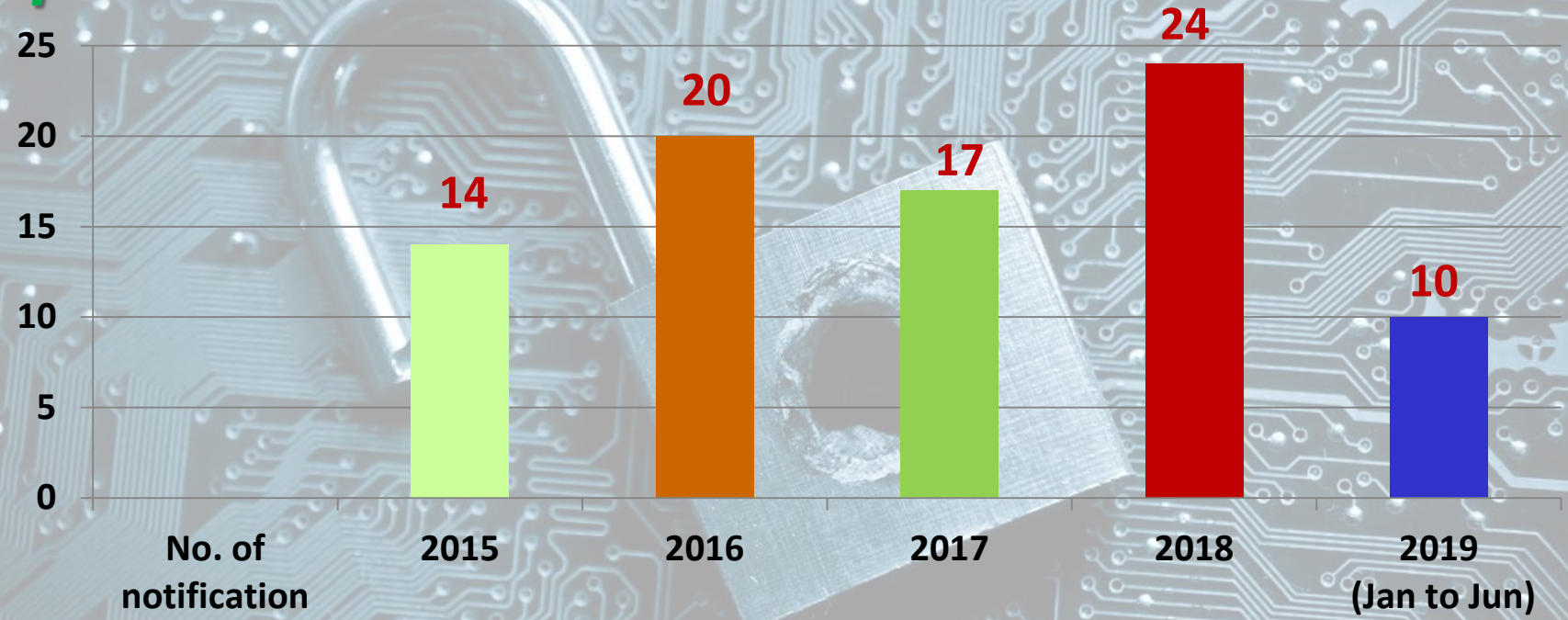
Distribution of cybersecurity incidents reported to HKCERT in 2018



Data breaches reported to PCPD 2013-2018 (voluntary)



Data breaches reported to PCPD by Government Departments 2013-2019



Paradigm shift from Compliance to *Accountability & Data Ethics*

Ethics, Laws, & Accountability

Extended obligation to ensure compliance with laws

Legal obligations, usually based on communal values

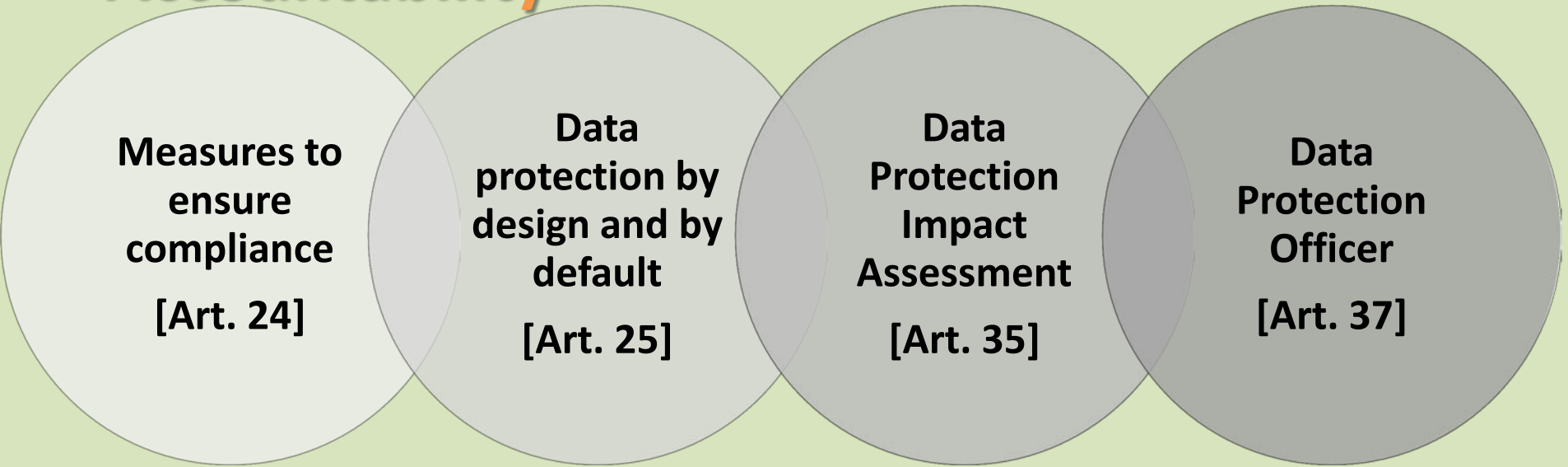
Communal values shared by the public in general, guiding our daily living

Accountability

Responsibility to put in place adequate policies and measures to ensure and demonstrate compliance

Rationale: Data users are in the best position to identify, assess and address the privacy risks of their activities

GDPR
- Accountability



Personal Data (Privacy) Ordinance, Chapter 486 of the Laws of Hong Kong (1995)

No general accountability requirement

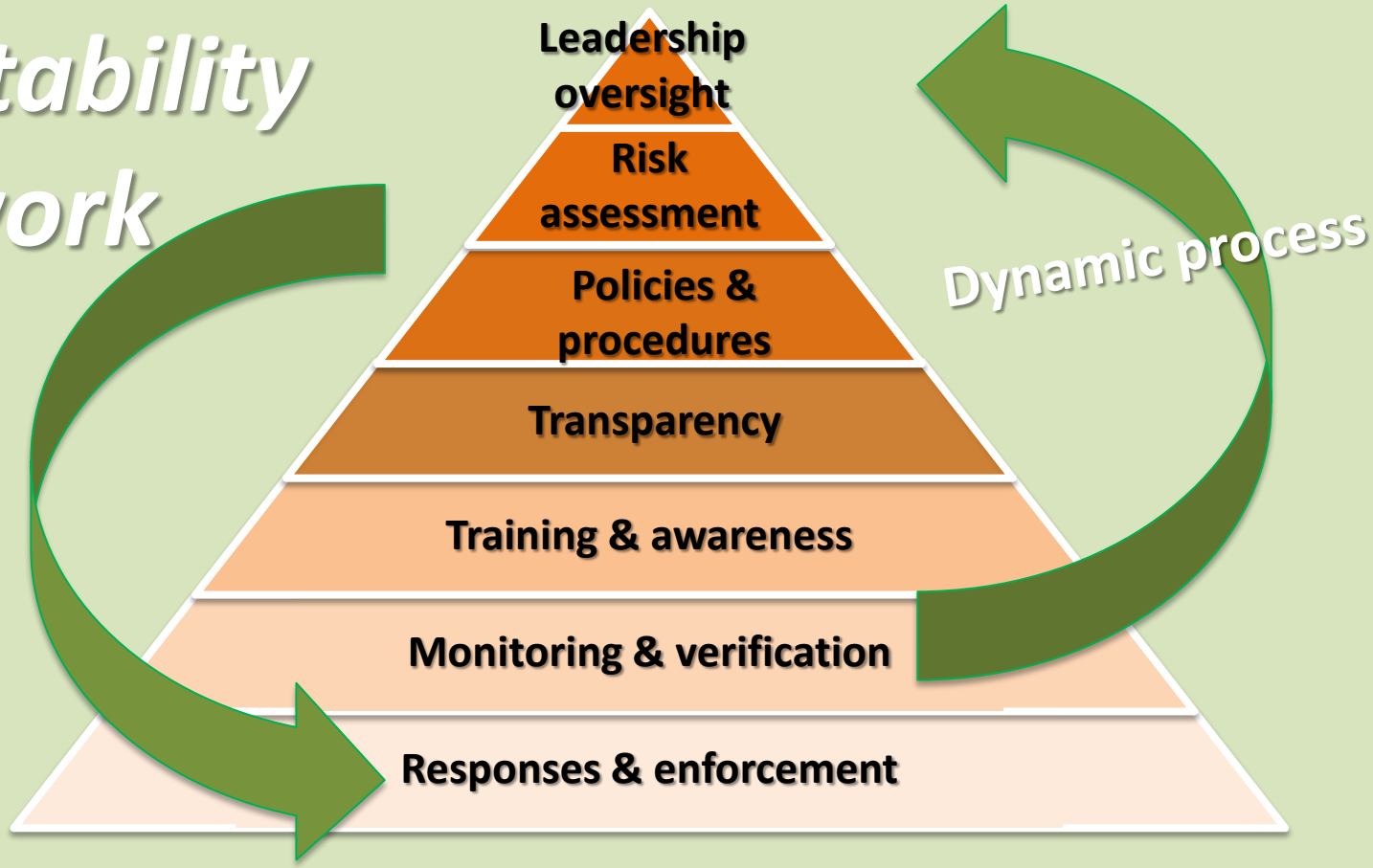
Some elements of accountability, i.e. "*all practicable steps*" shall be taken to ensure personal data is-

- **accurate [DPP 2(1)]**
- **not retained longer than necessary [DPP 2(2)]**
- **protected against data security incidents [DPP 4(1)]**

PCPD's Accountability Framework: Privacy Management Programme (PMP)

- **Voluntary accountability framework**
- **First published – February 2014**
- **First revision – August 2018**
- **Second revision – March 2019**
- **Pledged organisations:**
  - **All government bureaus and departments**
  - **37 commercial and public organisations** (e.g. insurance, telecommunications, transportation, heath care, public utilities)

Accountability framework



PMP – Main Components

1.1
Buy-in from the Top

1.2
Appointment of DPO

1.3
Establishment of Reporting Mechanisms

PMP – Main Components

2.1
Personal Data Inventory

2.2
Personal Data Policies

2.3
Risk Assessment Tools

2.4
Training, Education & Promotion

2.5
Handling of Data Breach

2.6
Data Processor Management

2.7
Communications

PMP – Main Components

3.1
Development of Oversight & Review Plan

3.2
Assessment & Revision of Programme Controls

Data ethics

A multi-stakeholder approach in personal data protection…

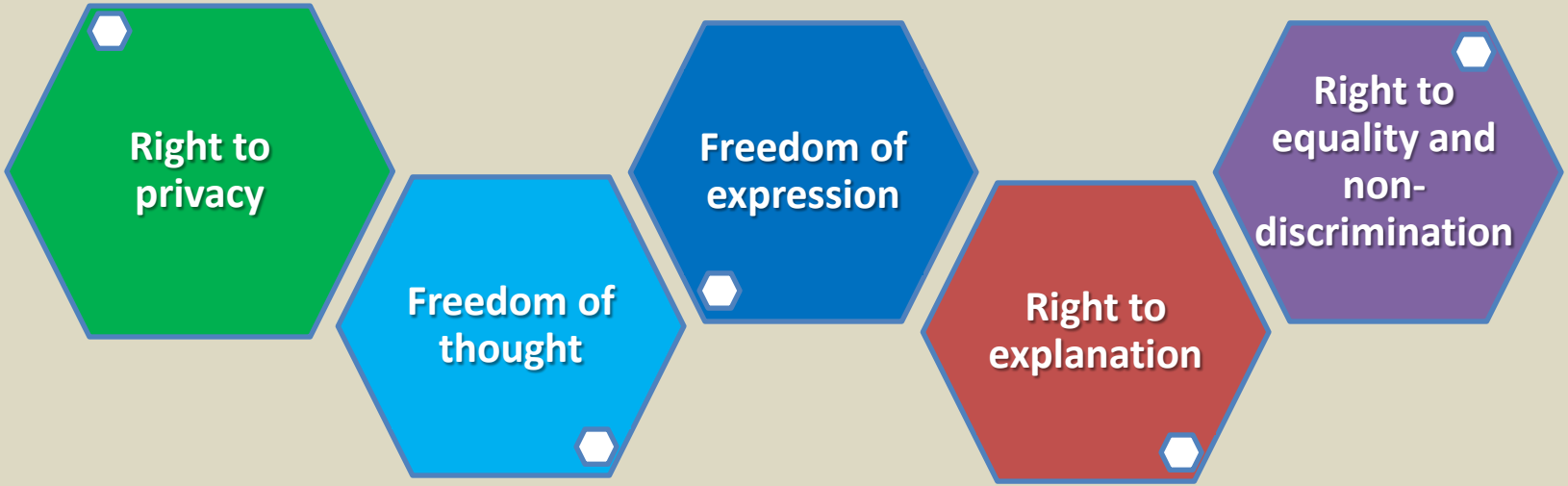
…with due consideration and respect for the rights and interests of all stakeholders, including individual data subjects and society as a whole

Data ethics

Re-emphasise conformity to ethical, communal values in the whole data lifecycle

Data ethics

Rights and interests of stakeholders include:



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

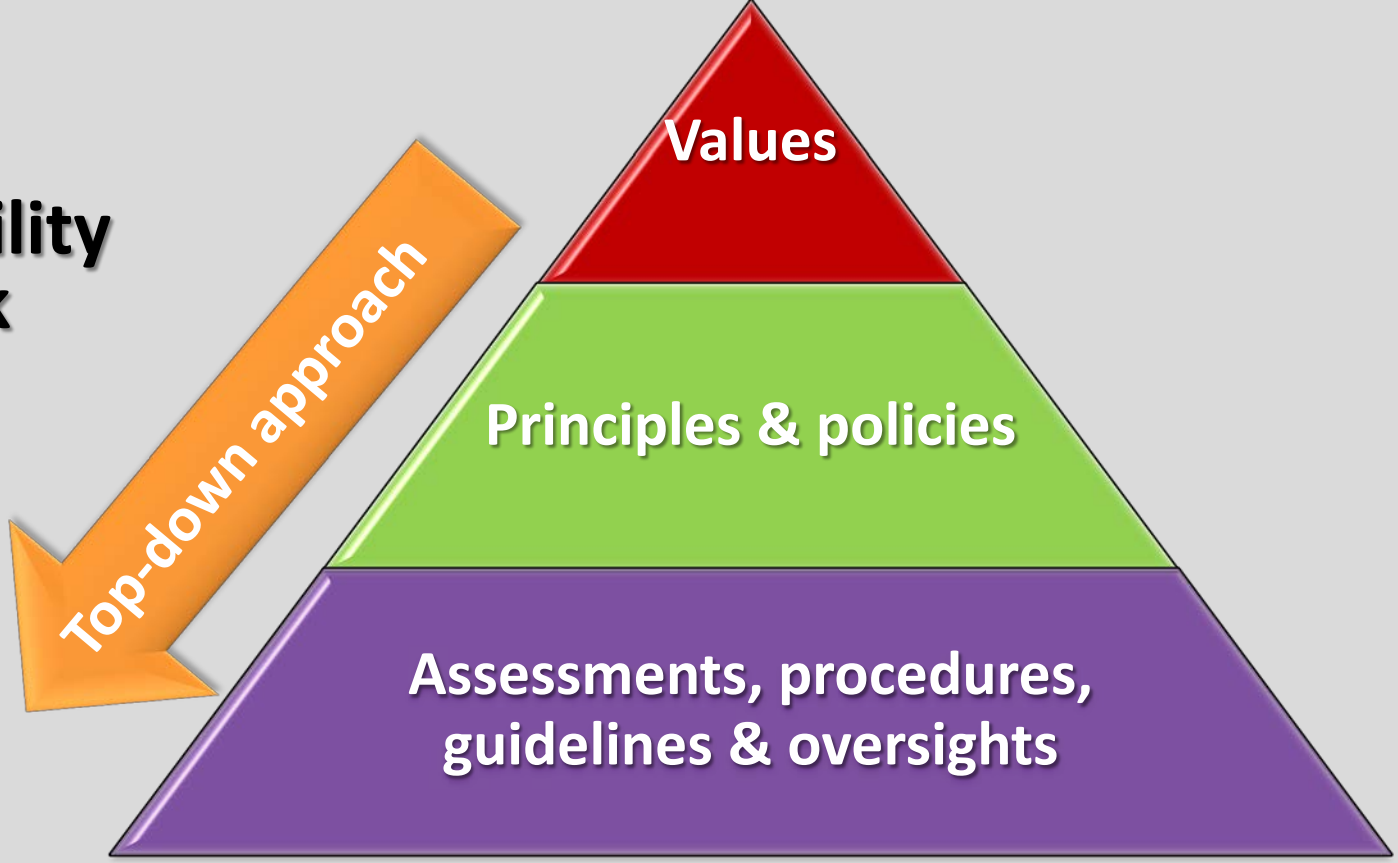
"***Ethics Guidelines for Trustworthy AI***" issued by the European Commission

Ethics on AI first discussed in Hong Kong (2017)

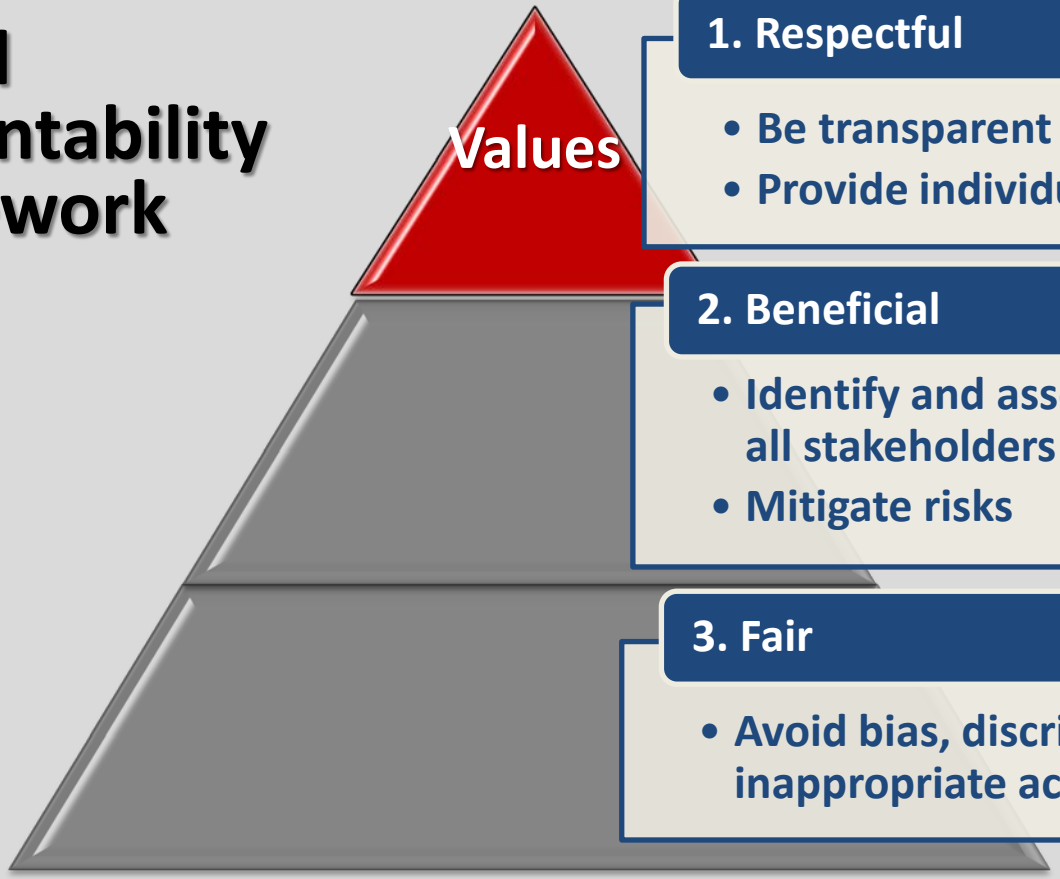
*"Data users need to add value beyond just complying with the regulations. Discussions about "**New Digital Ethics**", the relevant ethical standard and stewardship have already begun. Surely the deliberations will go on. In the not far away future, we may come up with an "**Equitable Privacy Right**"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

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

PCPD's Ethical Accountability Framework (2018)



Ethical Accountability Framework



1. Respectful

- Be transparent
- Provide individuals with control

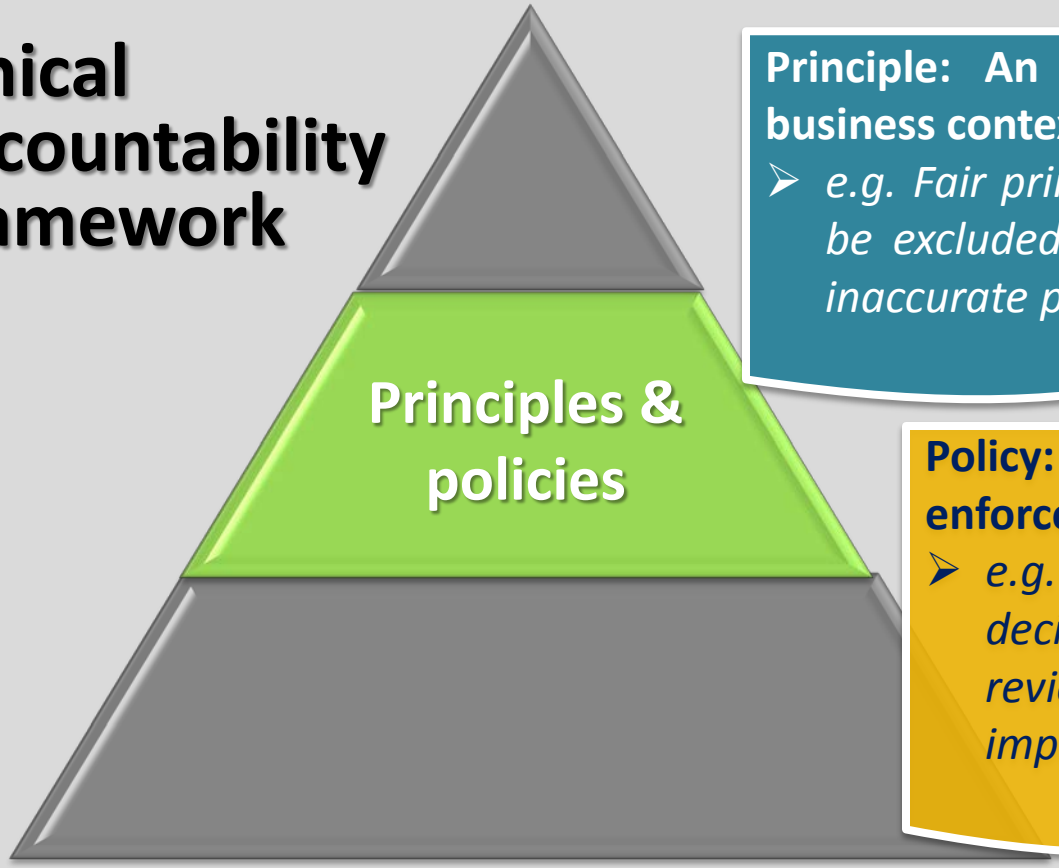
2. Beneficial

- Identify and assess risks and benefits to all stakeholders
- Mitigate risks

3. Fair

- Avoid bias, discrimination and other inappropriate actions

Ethical Accountability Framework



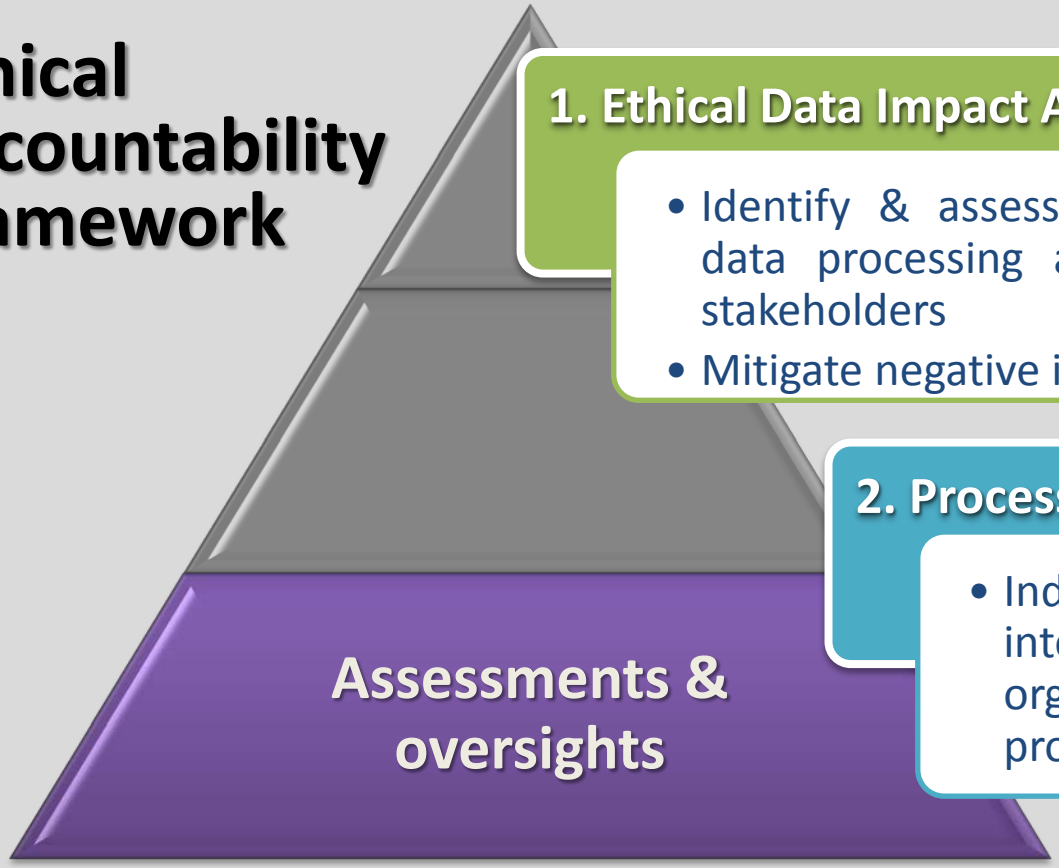
Principle: An expression of Values in business context

- *e.g. Fair principle: No customer should be excluded from banking services by inaccurate profiling and KYC*

Policy: Translation from Values into enforceable procedures

- *e.g. Fair policy: Automated decisions are subject to human review if they produce negative impact on customers*

Ethical Accountability Framework



1. Ethical Data Impact Assessment

- Identify & assess the impact of data processing activities on all stakeholders
- Mitigate negative impacts

2. Process Oversight

- Independent assessment on the integrity and effectiveness of an organisation's data stewardship programme

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

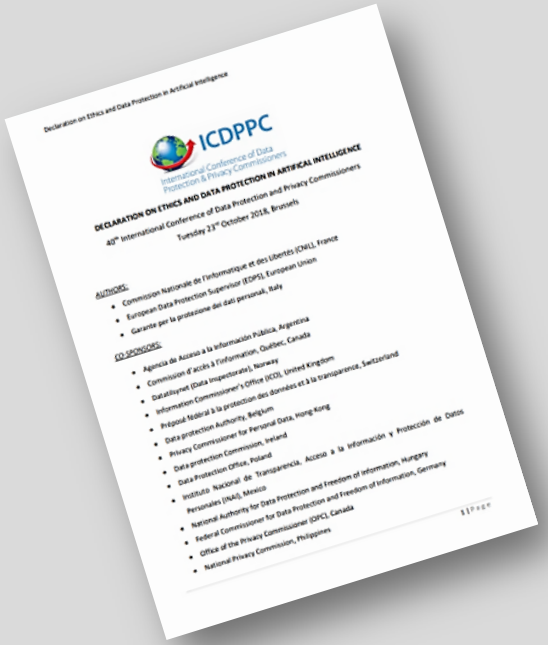
Step 3: Conduct impact assessment, i.e. risks and benefits to the individuals, the society and the organisation itself

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

Process Oversight – Questions to Consider

- Are the **accountability and responsibility** of data stewardship clearly defined?
- Are the core values translated into **principles, policies and processes**?
- Does the organisation adopt "**ethics by design**"?
- Are **Ethical Data Impact Assessments** properly conducted?
- Are **internal reviews** conducted periodically?
- Are there any **feedback and appeal mechanisms** for the individuals impacted ?
- Is there any mechanism to ensure the **transparency** of the data processing activities?

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



Fairness principle

Reducing biases or discriminations

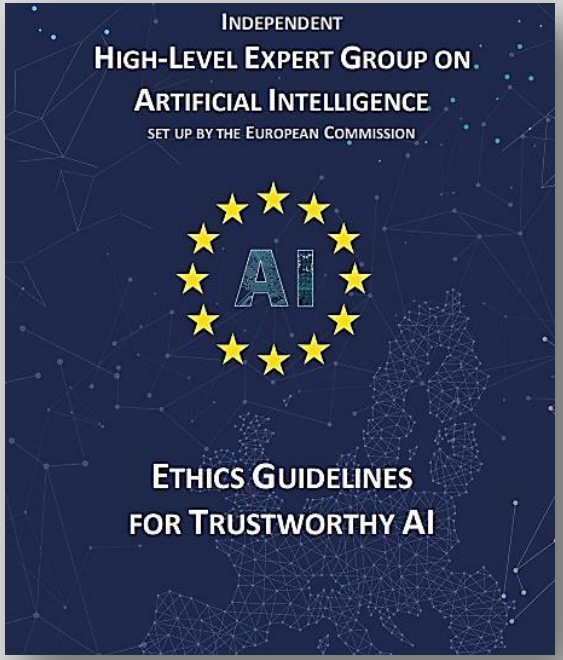
Continued attention and vigilance

Empowerment of every individual

Systems transparency and intelligibility

Ethics by design

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

Information Leaflet

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

PCPD.org.hk

Data Ethics for Small and Medium Enterprises

Preamble

In a data-driven economy, small and medium enterprises ("SMEs"), including tech start-ups, increasingly use personal data of customers as an asset in operating and advancing their businesses. The rapid development in information and communications technology, particularly advanced data processing activities (including big data analytics and artificial intelligence), present business opportunities but at the same time challenges privacy and data protection.

It is not in dispute that personal data belongs to the data subjects. SMEs that derive benefits from personal data should ditch the mindset of conducting their operations to merely meet the minimum regulatory requirements only. They should instead be held to a higher ethical standard that meets stakeholders' expectations alongside the requirements of laws and regulations. Data ethics can therefore bridge the gap between legal requirements and stakeholders' expectations.

In fact, ethical use of personal data makes good business sense. **Respectful**, **beneficial** and **fair** use of customers' personal data can improve business reputation and enhance stakeholders' confidence. This leaflet aims to help SMEs understand the means to implement data ethics. When SMEs develop an assessment process to ensure that personal data is processed ethically, individuals will have greater confidence in their data being protected. In turn, customers' trust will grow and become a competitive edge of the SMEs. Under the trend of service and product personalisation and mobilisation in the future smart society, enterprises will benefit by grasping and implementing data ethics.

Three Core Values of Data Ethics

SMEs are encouraged to handle personal data pursuant to three core values, namely being **Respectful**, **Beneficial** and **Fair**.

Respectful[1]

- SMEs should be accountable for conducting advanced data processing activities
- SMEs should consider the expectations of the individuals to whom the data relate and/or impacted by the data use
- SMEs should consider all parties that have interests in the data
- Decisions made about an individual and the relevant decision-making process should be explainable and reasonable
- Individuals should be able to make inquiries, obtain explanation and appeal against decisions on the advanced data processing activities that impact them

1 The Respectful value is consistent with Data Protection Principles (**DPPs**) 1, 3, 5 and 6 in Schedule 1 to the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong).

Data Ethics for Small and Medium Enterprises 1 April 2019

PCPD information leaflet

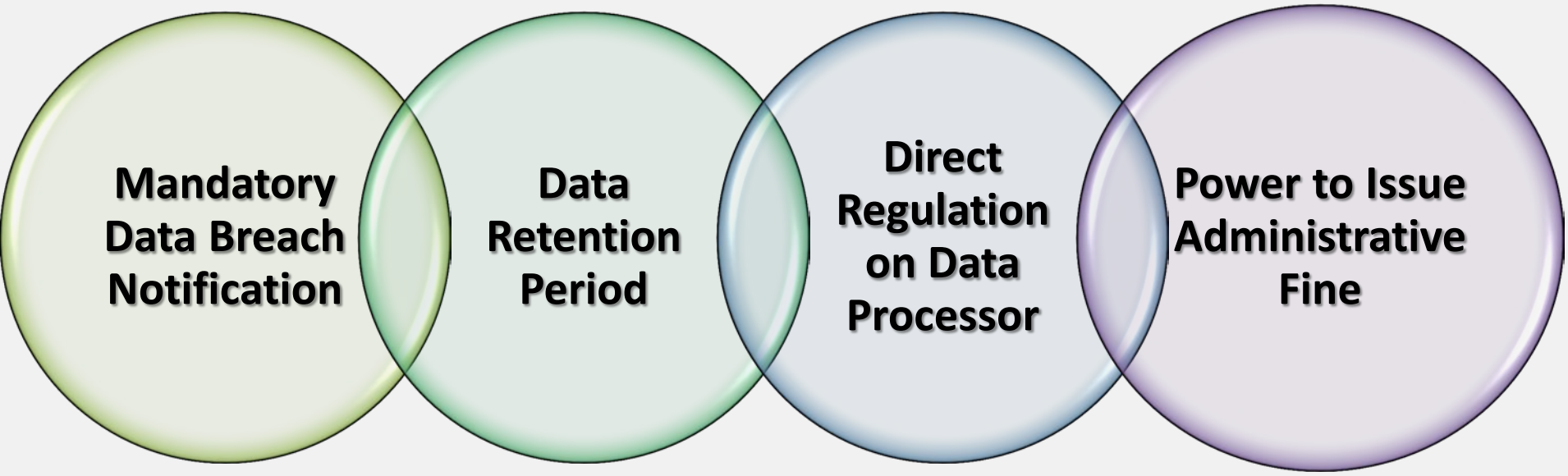
Data Ethics for Small and Medium Enterprises

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

Review of the PDPO

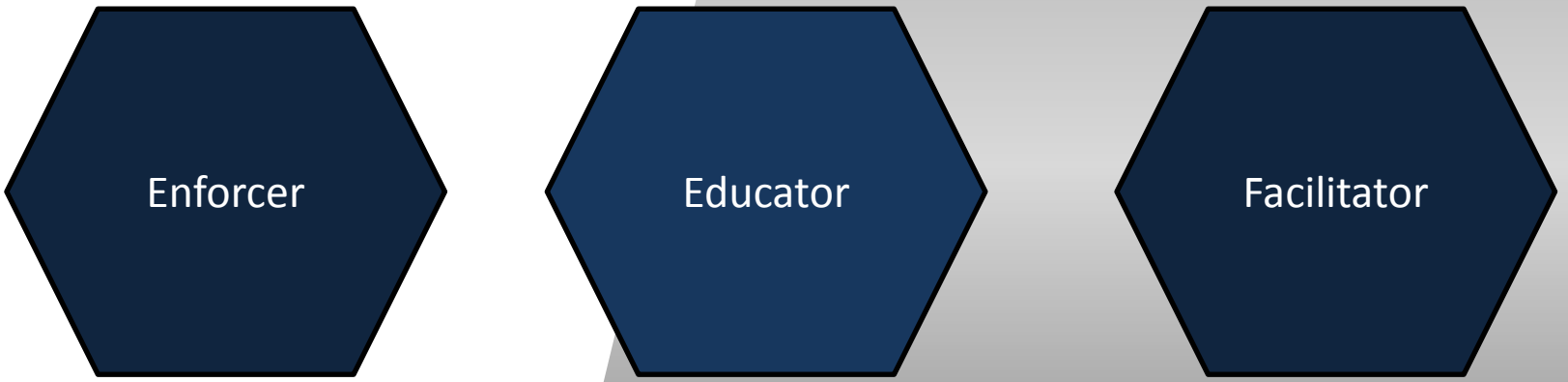


Incentivising & Engaging

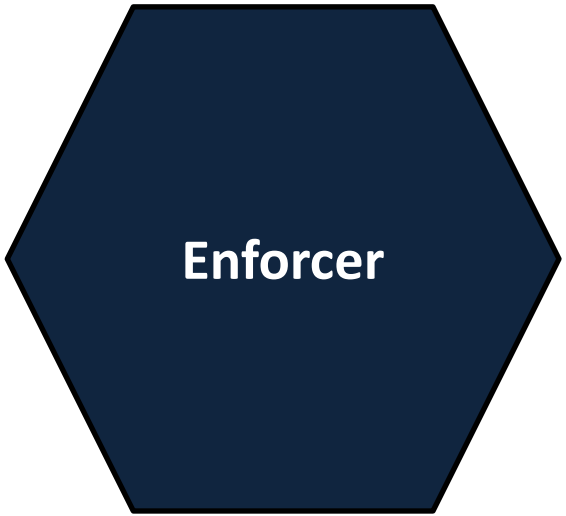
Core values of personal data protection

- Personal data privacy right is a fundament 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

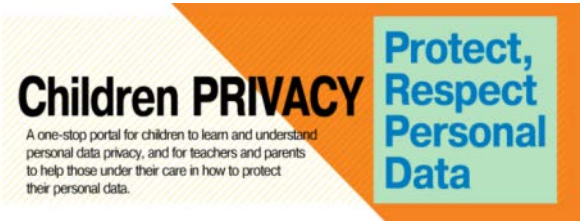
Regulating for Results

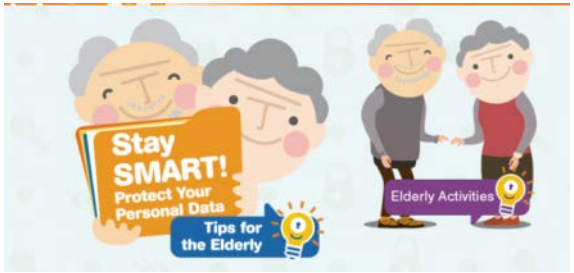


Fair enforcement, taking into account



- 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


Stay SMART!
Protect Your Personal Data
Tips for the Elderly
Elderly Activities


Student Ambassador Programme
學生大使活動
2018
保障私隱 學生大使 · 學校夥伴嘉許計劃 2018

Educator

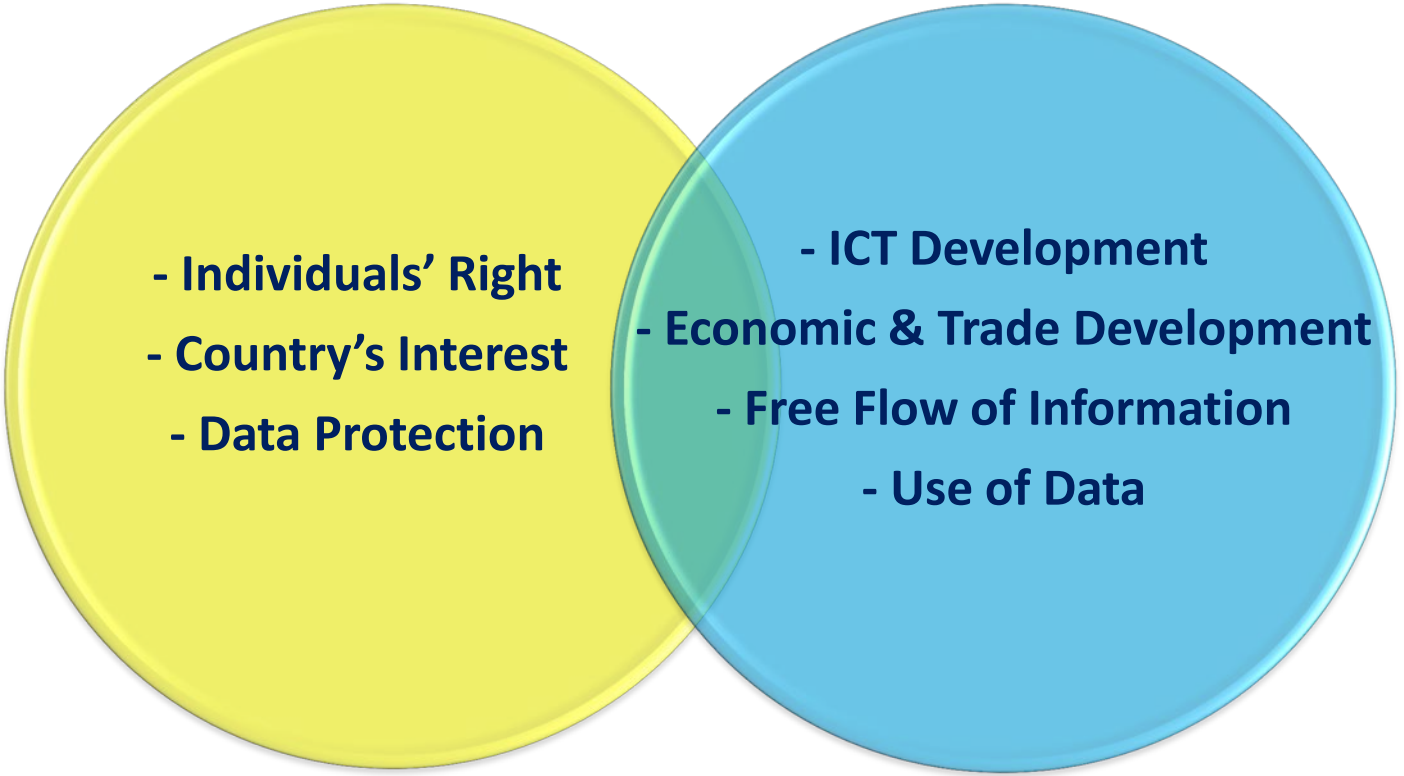
Education campaigns in 2018

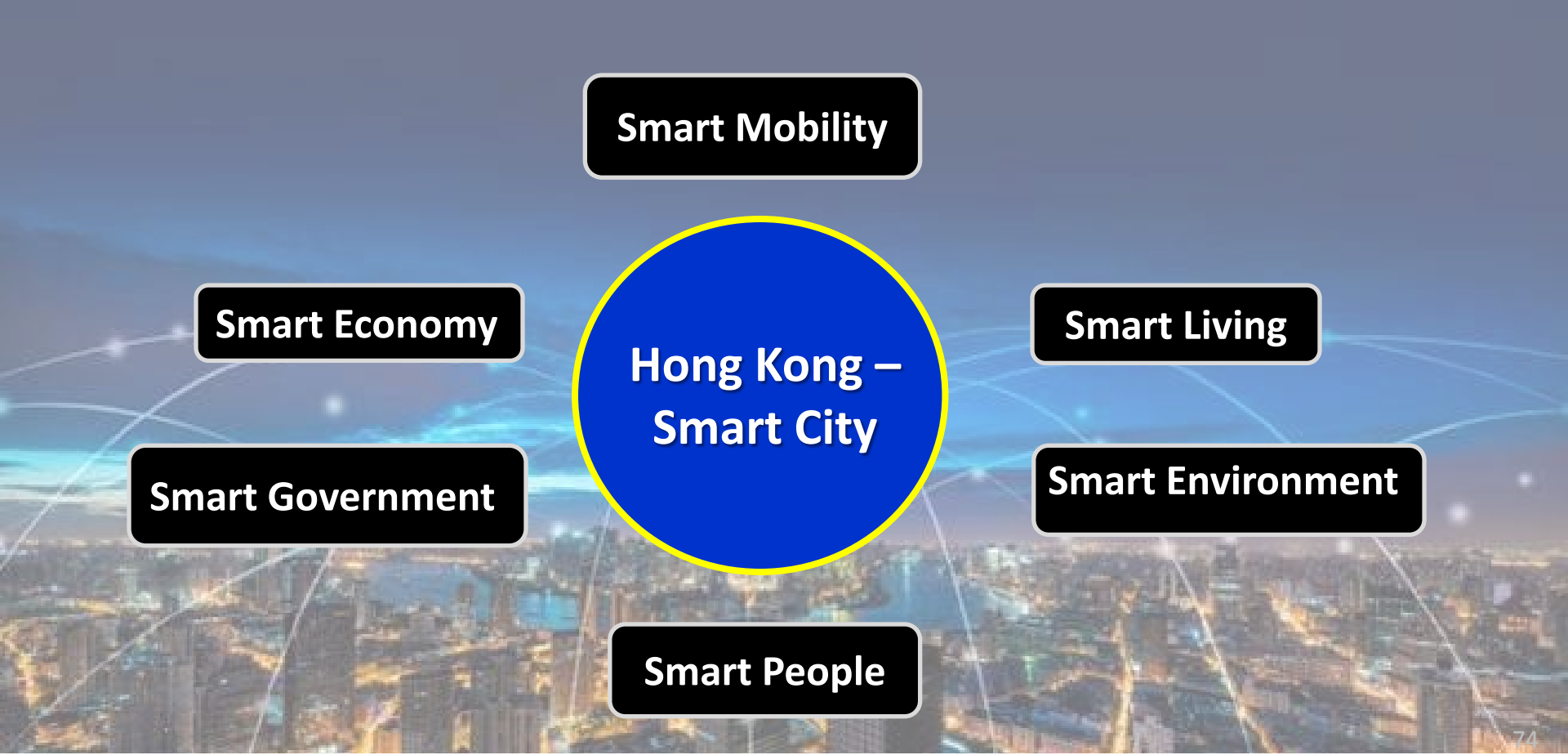
- 18 promotional and education programmes with 262,145 participants
- 106 schools joined “Student Ambassador for Privacy Programme”
- 421 professional workshops, talks and seminars

Facilitator

Lawful, accountable and ethical use of personal data

A Balancing Exercise




Smart Mobility
Smart Economy
Hong Kong – Smart City
Smart Living
Smart Government
Smart Environment
Smart People

Wi-Fi Connected City

Intelligent Transport System and Traffic Management

eID

Big Data Analytics Platform

FinTech

Hong Kong Smart City Initiatives

Smart Tourism

Multi-functional Smart Lampposts

Open Data

Digital Payment

Source: Hong Kong Smart City Blueprint

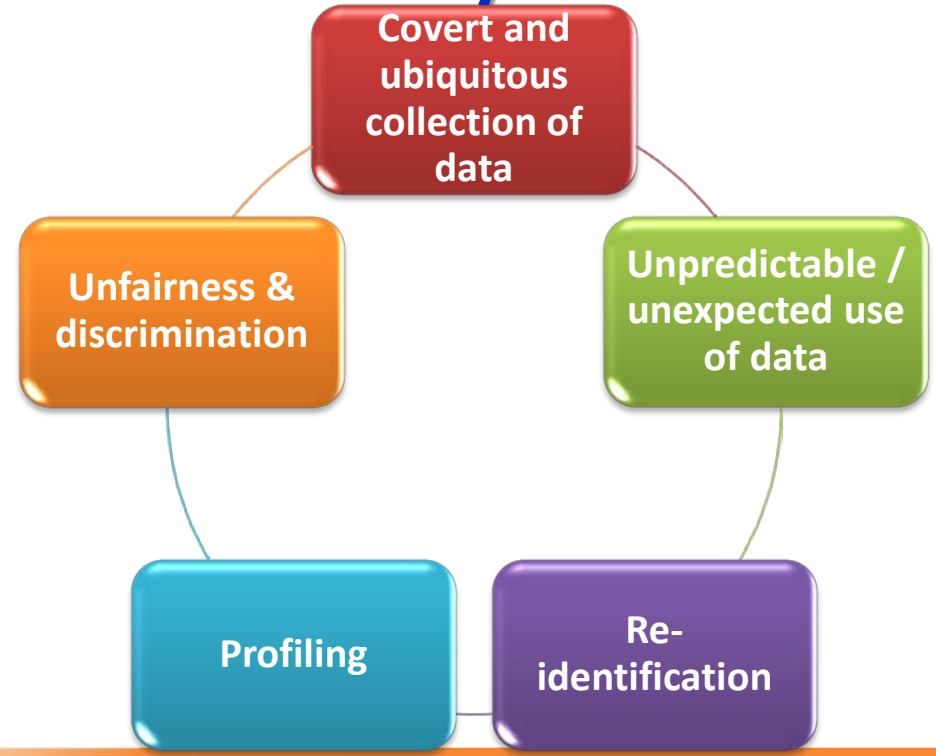
Government Open Data

Government's first annual open data plans: over 650 new datasets will be released in 2019

By the end of 2019, the number of datasets available: around 3,300 → 4,000

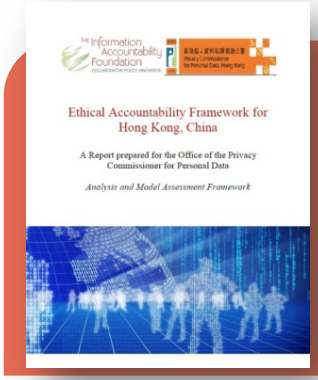
Bureaux and departments should endeavour to release their data for free public use

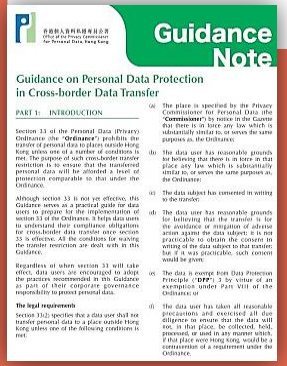
Privacy Concerns about Use of ICT and Big Data in Smart City Initiatives



Treat Data as Money

Download our publications:





Contact Us

- 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