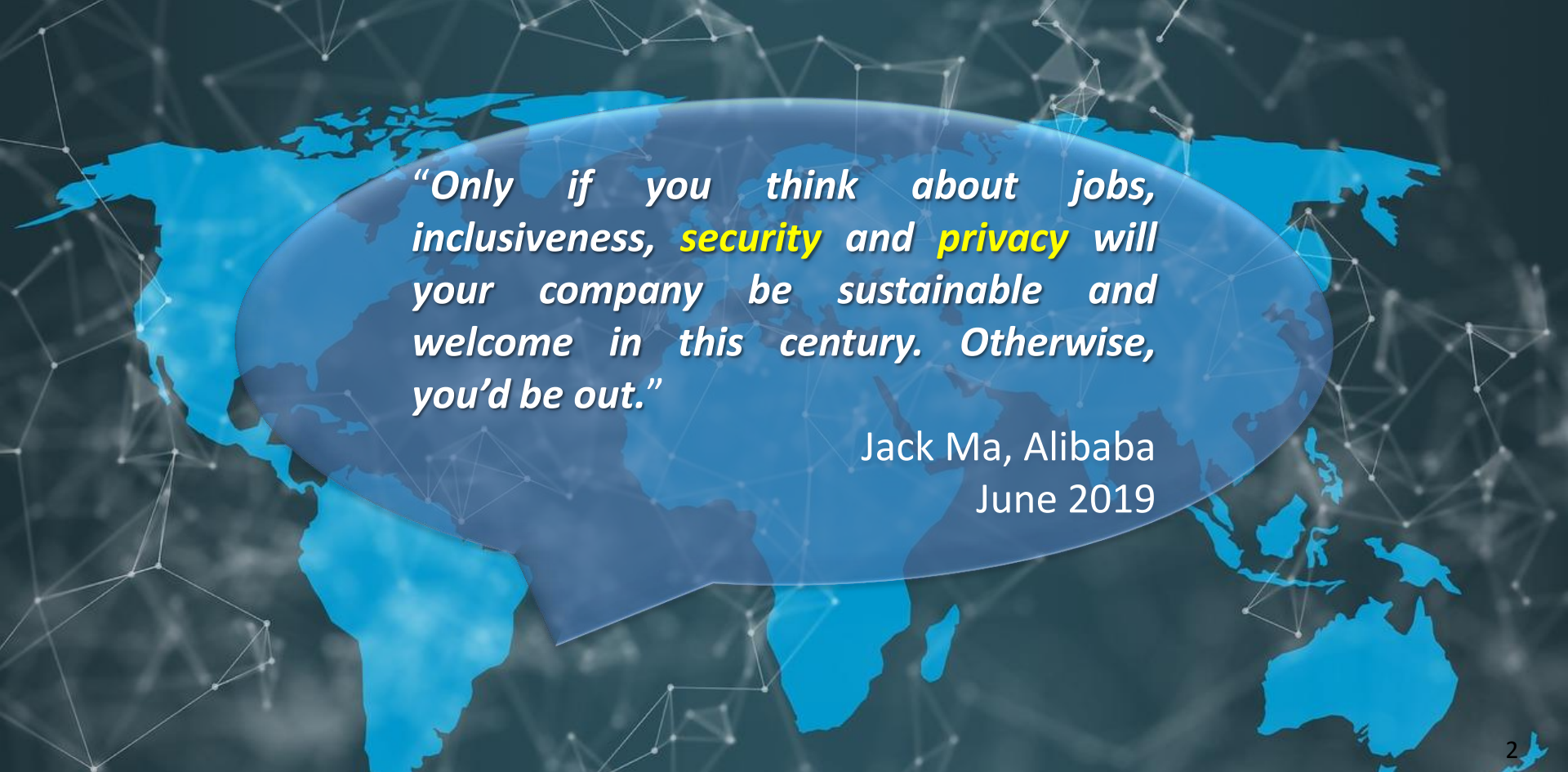


# MWC19 Shanghai - Data Trust & Security Summit

28 June 2019 | Shanghai, China

## Data Security, Privacy & Trust: The Three Cornerstones of Digital Ecosystem

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



*“Only if you think about jobs, inclusiveness, **security** and **privacy** will your company be sustainable and welcome in this century. Otherwise, you’d be out.”*

Jack Ma, Alibaba  
June 2019

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



Microsoft – IDC Study:  
Understanding Consumer  
Trust in Digital Services  
in Asia Pacific



- 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 2019)

- **Only 31% of consumers trust organisations offering digital services to protect their personal data**
- **More than 50% of consumers will switch to another organisation in the event of negative trust experience, such as breach of security and privacy**



# Digital Ecosystem

Accountability

Ethics

Data  
Security

Data  
Privacy

# Publicised data breach 2018 (global)

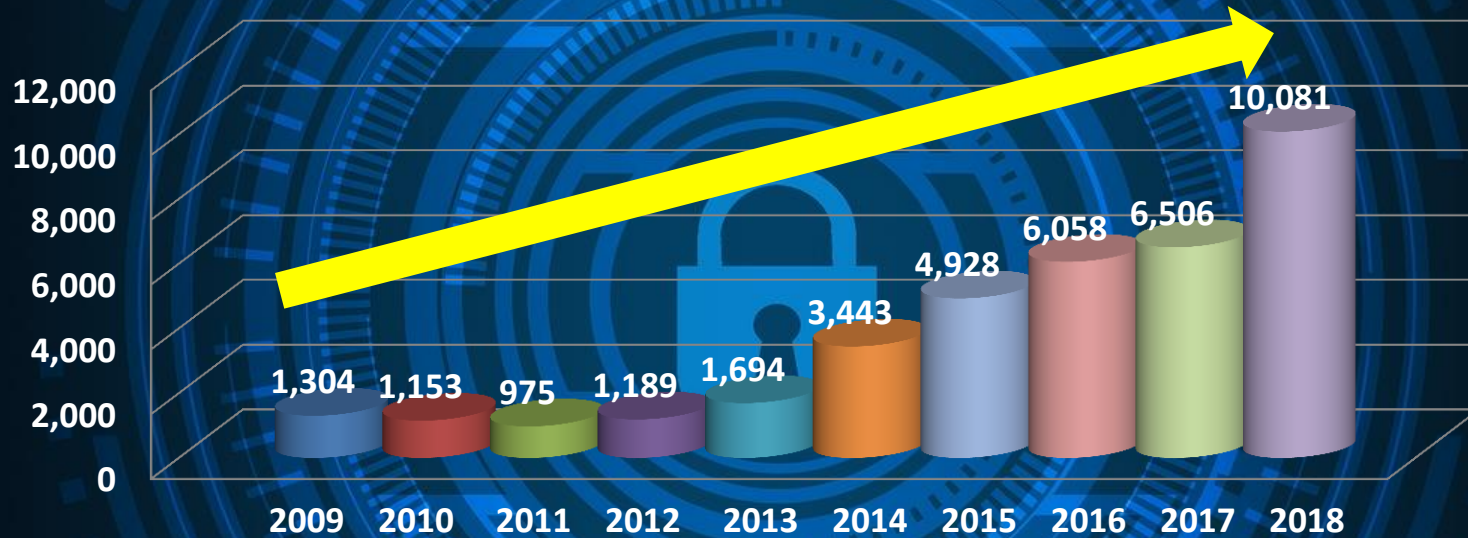
- 6,515 breaches
- 5 billion records



Top 5 breach types

Source: Risk Based Security

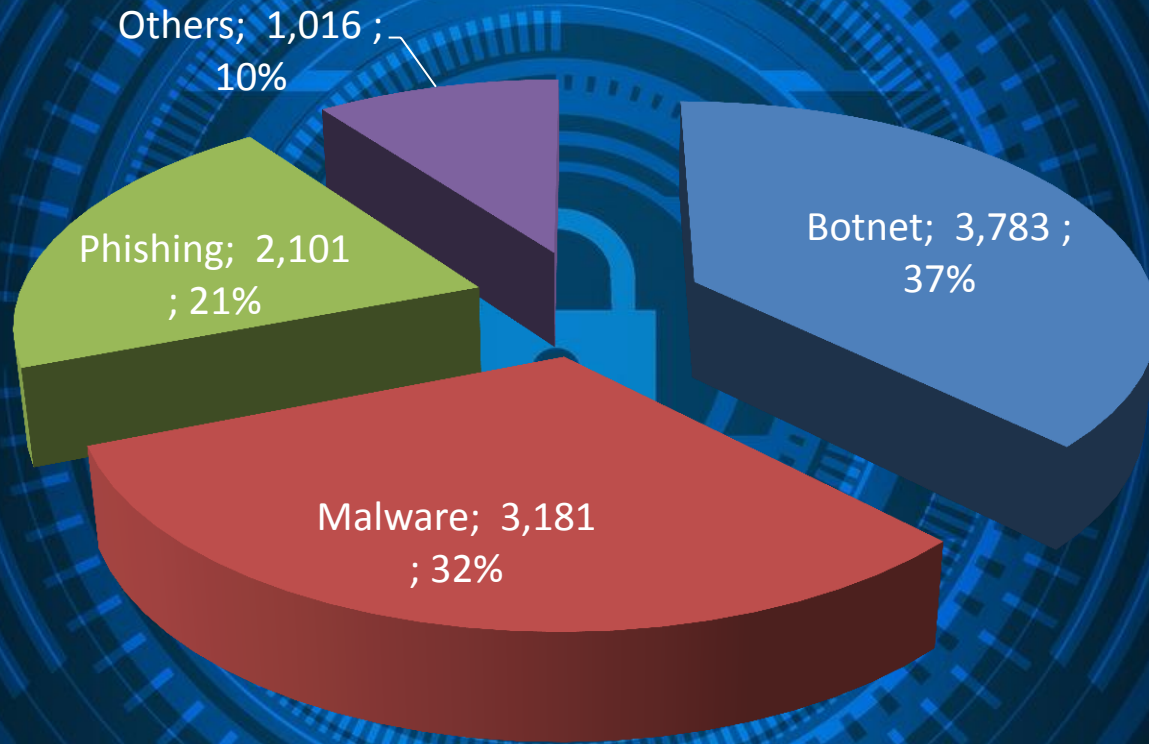
# Cybersecurity incidents reported to HKCERT 2009-2018



Source: HKCERT

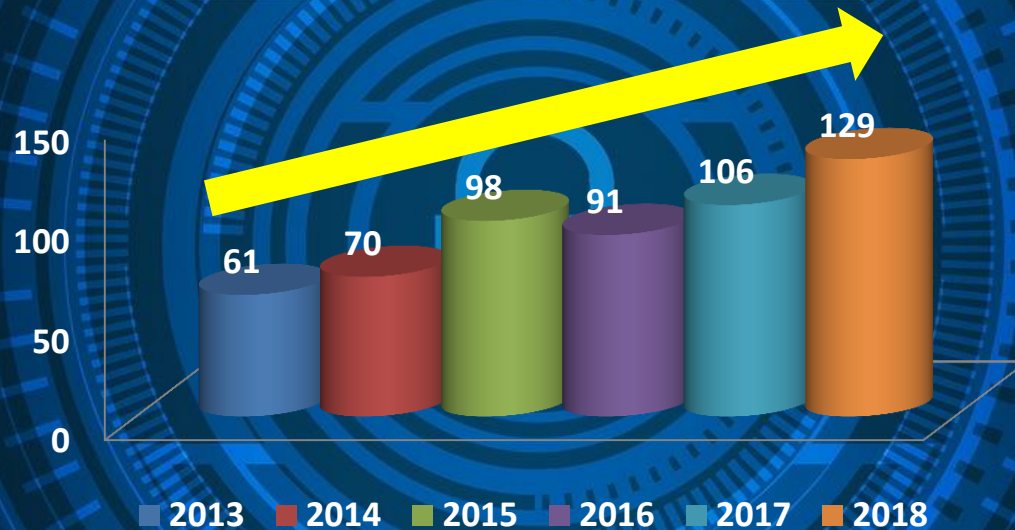


# Distribution of cybersecurity incidents reported to HKCERT in 2018



Source: HKCERT

# Data breaches reported to PCPD 2013-2018 (voluntary)





# Data security – *The pressing issues*

IT is increasing  
integrated  
into business  
operations

Increase in  
sophistication  
of hackers  
(Hacking as a  
Service, or  
HaaS,  
emerges)

Cyberattack is  
not “if” but  
“when”

# Case study:

## *Data breach of an airline based in HK affecting 9.4m passengers*

### Background

- Data breach notification lodged to PCPD on 24 Oct 2018
- Unauthorised access to airlines information systems
- 9.4 million passengers from over 260 countries / jurisdictions / locations affected
- Personal data involved consisted mainly of name, flight number and date, email address, membership number, address, phone number

# Case study:

## *Data breach of an airline based in HK affecting 9.4m passengers*

### PCPD's investigation and findings

Investigation  
focuses

Data security

Data retention  
period

Contraventions

Various data security failures (see next slides)

Not taking all reasonably practicable steps to erase unnecessary HK Identity Card No. of passengers



# Case study:

## *Data breach of an airline based in HK affecting 9.4m passengers*

### Date security failures include:

- Risk alertness being low
- Vulnerability scanning exercise at a yearly interval (too lax)
- Failure to identify and address the commonly known exploitable vulnerability
- Failure to have an effective personal data inventory
- Failure to apply effective multi-factor authentication to all remote access users

Corporate  
governance failure

Risk assessment  
failure

Operational  
measure failure

Technical measure  
failure

# Case study:

## *Data breach of an airline based in HK affecting 9.4m passengers*

### PCPD's enforcement action

### **Enforcement Notice**

Engage independent data security expert to overhaul systems

Implement effective multi-factor authentication for remote access

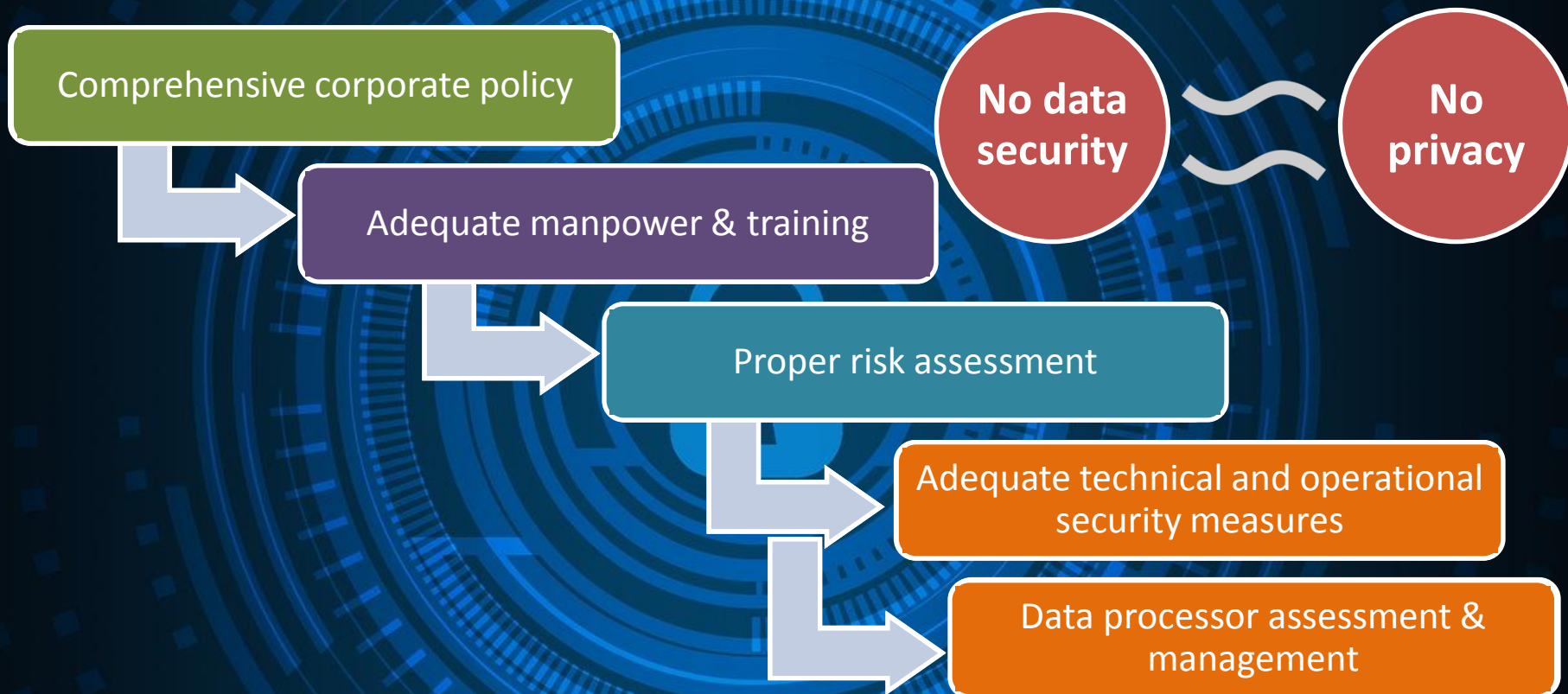
Conduct effective vulnerability scans

Engage independent data security expert to review / tests system security

Devise clear data retention policy, specify retention period(s) and ensure effective execution

Completely obliterate all unnecessary HKID Card numbers

# Data security – ‘All practical steps’ approach





# Data privacy – *The pressing issues*

**Big data analytics  
& AI**

- Re-identification
- Lack of transparency
- Bias & discrimination
- Loss of control by individuals

# Data privacy

## – *Emerging regulatory responses*

Expanded scope of personal data

Increased obligations and sanctions of data users

Enhanced rights of individuals

Accountability & ethics

# Data privacy – What is ‘personal data’?

## EU approach

- Data

*relating* to

an **identifiable** individual

Take into account all possible means likely to be used

- Includes *location data & online identifiers*

Broadened  
scope

Stronger  
privacy  
protection

# Privacy



# Data privacy

## – *Enhanced rights and obligations in EU* (*and being replicated in other jurisdictions*)

### Individuals

- Enhanced right to notice
- Right to be forgotten
- Right to data portability
- Right to object to automated decision

### Data users

- Mandatory data breach notification
- **Accountability**
- Administrative sanctions

# Data privacy

## – Increasing regulation in mainland China

Cyber-security Law (2016)

General Provisions of the Civil Law (2017)

Personal Information Security Specification (2017) (now under revision)

E-Commerce Law (2018)

Data Security Management Measures (2019) (draft)

# Data privacy

## – *Increasing regulations in the world*

1973

1<sup>st</sup> privacy law  
enacted in Sweden

1973-2019

On average 2.9  
countries enacted  
privacy laws each  
year

April 2019

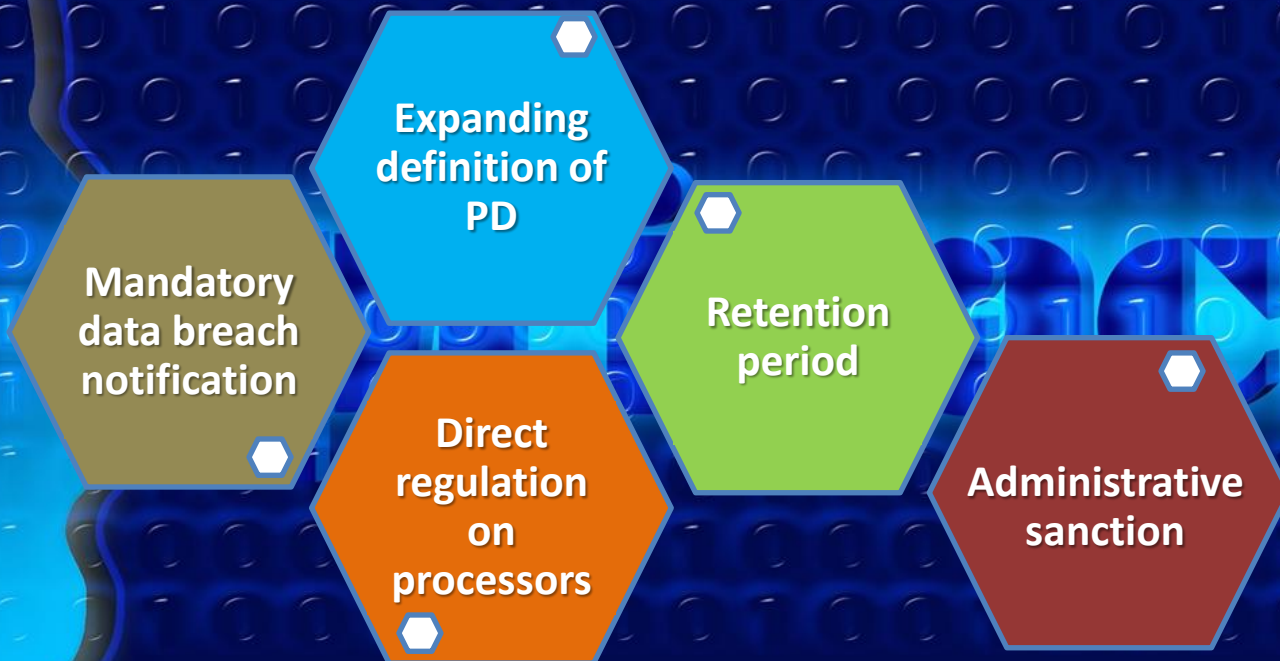
134 countries /  
regions with privacy  
laws

*Source: Graham Greenleaf*



# Data privacy

## – Possible reform in Hong Kong



# Paradigm shift from compliance to *accountability*

Translates legal requirements into  
**risk-based, verifiable and enforceable**  
corporate practices and controls



# Accountability

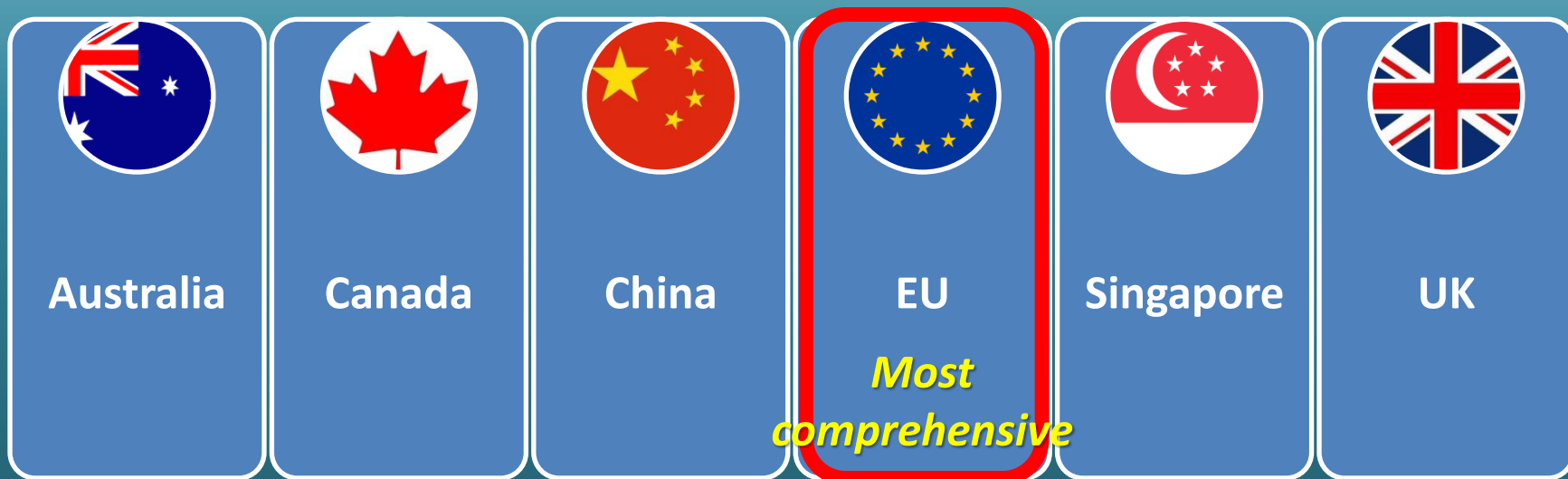
***Responsibility to put in place adequate policies and measures to ensure and demonstrate compliance***

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



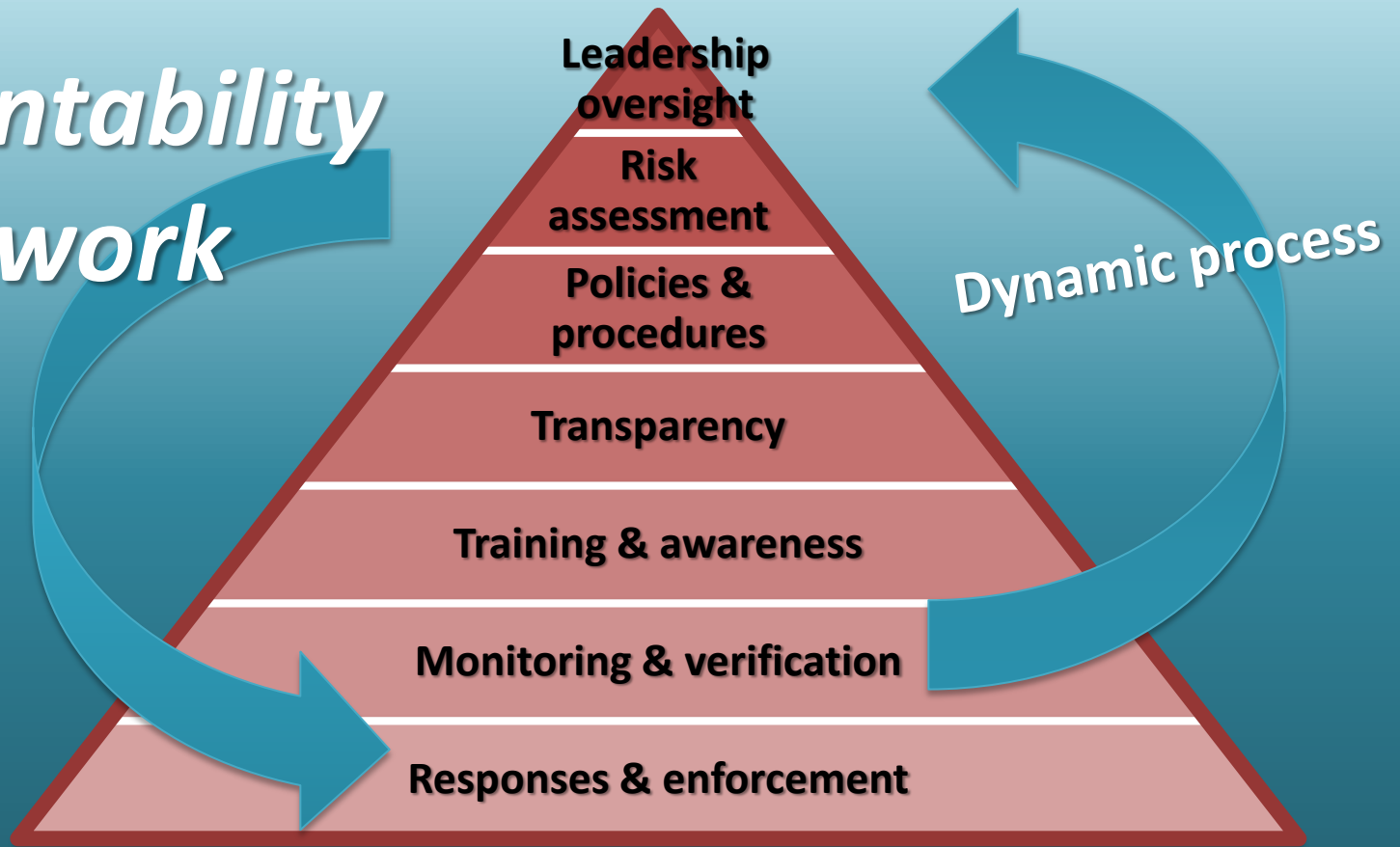
# Accountability

Examples of jurisdictions with accountability principles or elements of accountability embedded in data protection laws:



24

# Accountability framework



Source: CIPL

# *Accountability under EU GDPR*

Ensure &  
Demonstrate  
Compliance

Privacy by  
Design & by  
Default

Data  
Protection  
Officer

DP Impact  
Assessment

Records of  
Processing

*See GDPR articles 24, 25, 30, 35, 37-39*



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



Effective management of  
personal data



Minimisation of privacy  
risks



Effective handling of data  
breach incidents



Demonstrate compliance and  
accountability

<https://www.pcpd.org.hk/pmp/index.html>

# PMP – Main Components



## 1. Organisational Commitment

**1.1**  
Buy-in from the  
Top

**1.2**  
Appointment of  
DPO

**1.3**  
Establishment of  
Reporting  
Mechanisms

# PMP – Main Components



## 2. Programme Controls

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. Ongoing Assessment and Revision

3.1

Development of Oversight &  
Review Plan

3.2

Assessment & Revision of  
Programme Controls

# Ethics and Trust

*“Our customers’ trust means everything to us. We spent decades working to earn that trust.”*

Tim Cook, Apple  
August 2015

**Trust  
deteriorating?**

*“Our data is being weaponised against us.”*

Tim Cook, Apple  
October 2018

# 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)

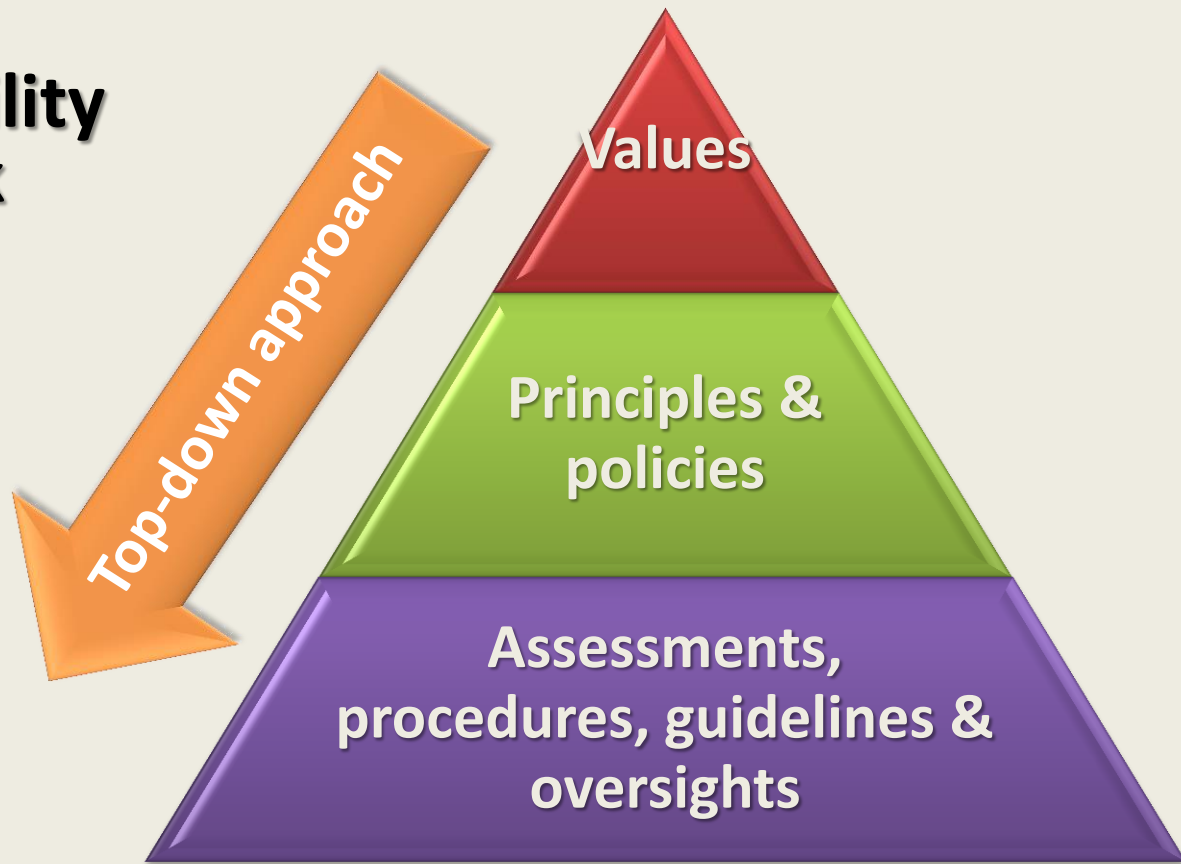


*“Data users need to add value beyond just complying with the regulations. Discussions about **“New Digital Ethics”**, the relevant ethical standard and stewardship have already begun. Surely the deliberations will go on. In the not far away future, we may come up with an **“Equitable Privacy Right”**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

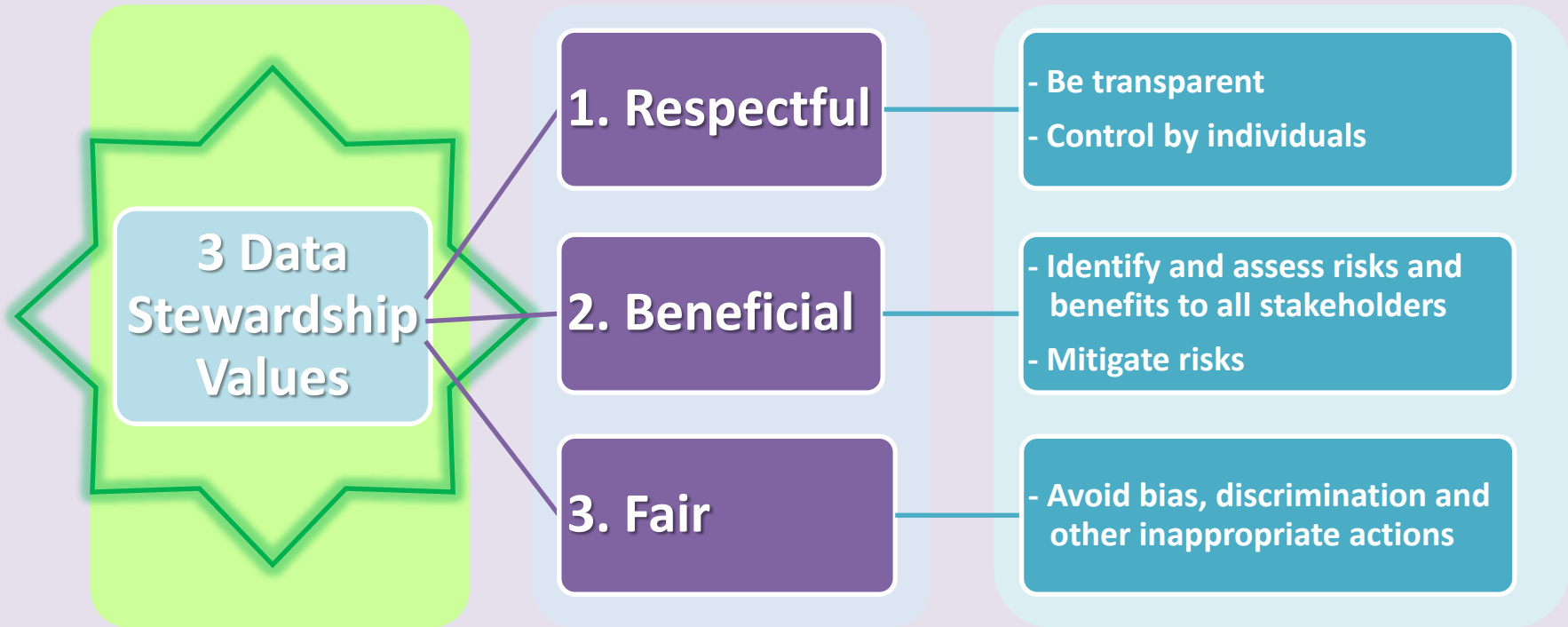
Stephen Kai-yi Wong  
Opening speech at 39<sup>th</sup> ICDPPC (2017)



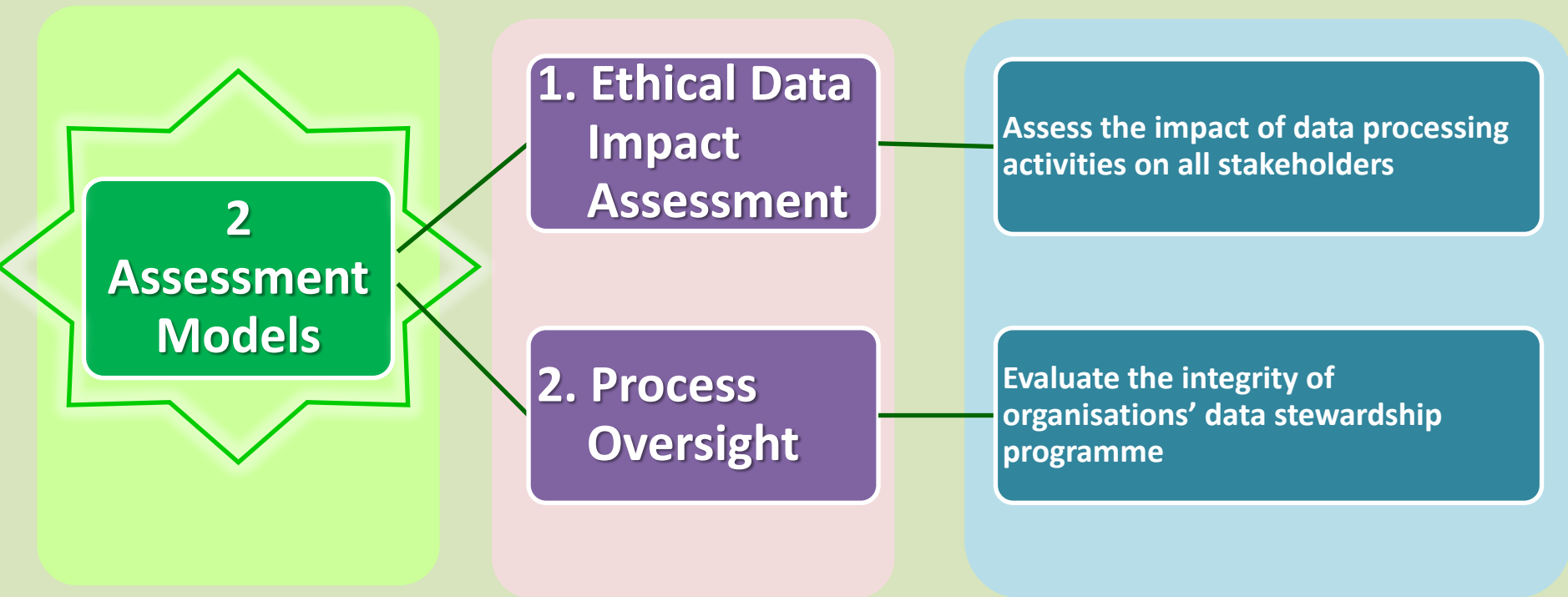
# Ethical Accountability Framework



# Multi-stakeholders Approach – Three Core Values



# Multi-stakeholders Approach – Two Assessment Models



# 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 (October 2018): Six Core Principles



Reducing  
biases or  
discriminations

Empowerment  
of every  
individual

Fairness  
principle

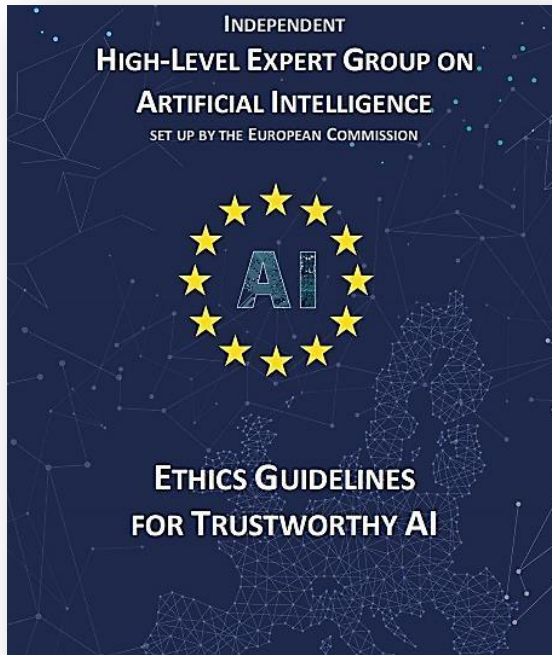


Continued  
attention  
and vigilance

Systems  
transparency  
and  
intelligibility

Ethics by design

# 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

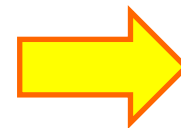
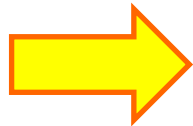
# PCPD's Roles – Enforcer + Educator + Facilitator

## PCPD's Strategic Focus

Fair Enforcement

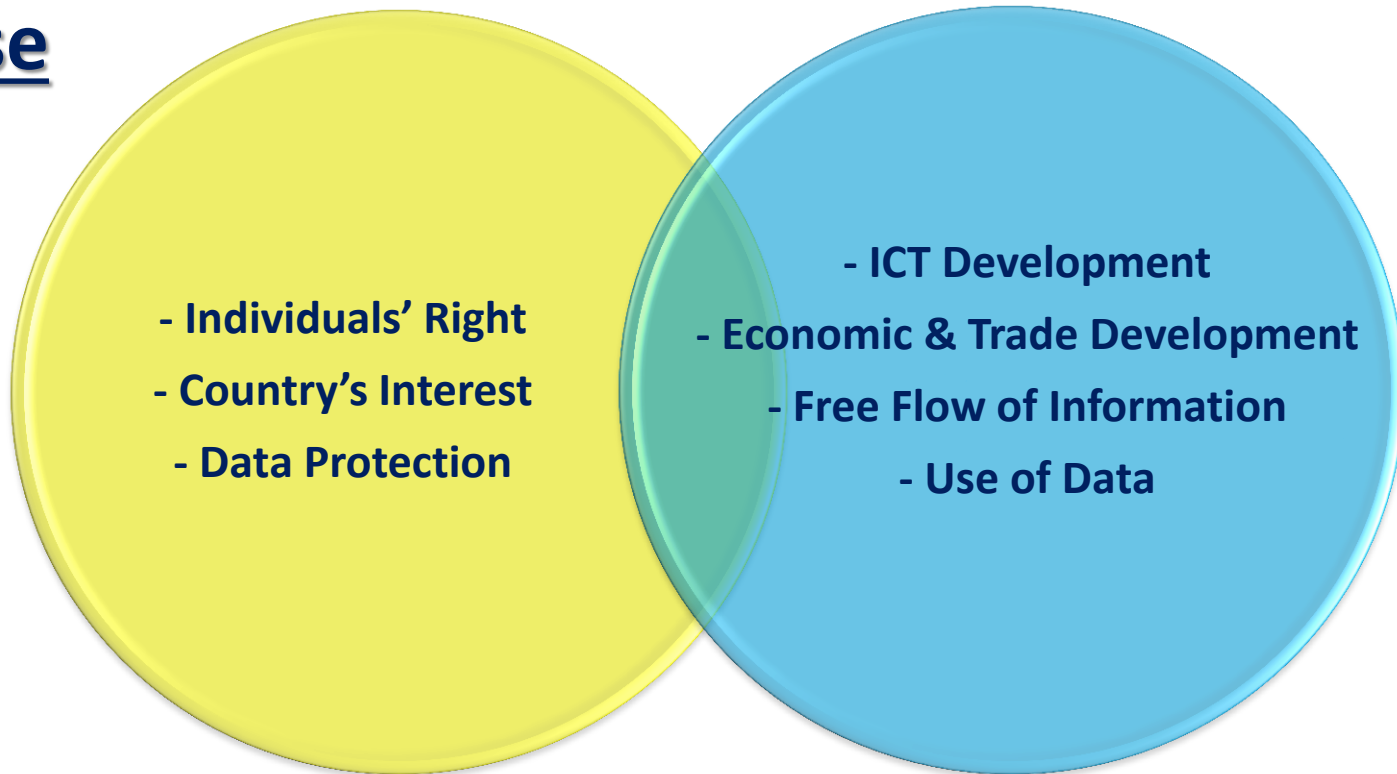
Engaging

Incentivising



**Privacy-friendly Culture**

# A Balancing Exercise





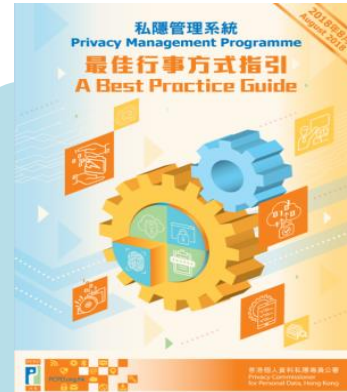
# Download our publications



## Ethical Accountability Framework for Hong Kong, China

A Report prepared for the Office of the Privacy Commissioner for Personal Data

*Analysis and Model Assessment Framework*



# Contact Us

The screenshot shows the PCPD website interface. At the top, there are navigation links for 'About PCPD', 'Data Privacy Law', 'News & Events', 'Compliance & Enforcement', 'Complaints', 'Legal Assistance', 'Education & Training', 'Resources Centre', and 'Enquiry'. Below this is a search bar with 'Hot Search', 'Advanced Search', and 'Keyword Search' options. The main content area features a 'What's New' section with several news items, including 'Reduce Cyberbullying by Nurturing Culture of "Protect, Respect Personal Data"', 'Privacy Commissioner Prize in Privacy and Data Protection Law 2017/18 to Recognise Student's Outstanding Performance in Study of Personal Data Privacy Protection', 'Respect Customers' Rights of Personal Data Self-determination Follow Their Opt-out Requests in Direct Marketing', 'Privacy Commissioner Completed Compliance Check on Facebook and Cambridge Analytics Incident', 'Privacy Commissioner Issues Best Practice Guide on Privacy Management Programme and Encourages Organisations to Embrace Personal Data Protection as Part of Corporate Governance Responsibilities', 'Unleashing Potential in Innovation and Technology - Promoting Data Privacy Protection Award Presentation Ceremony of Student Ambassador for Privacy Protection Programme', and 'Privacy Commissioner Expresses Concerns Over Typeform's Data Breach Incident (Chinese Version Only)'. There are also links for 'For Individuals' and 'For Organisations'. The 'A Quick Guide' section is highlighted with a blue arrow.

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](https://creativecommons.org/licenses/by/4.0).

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