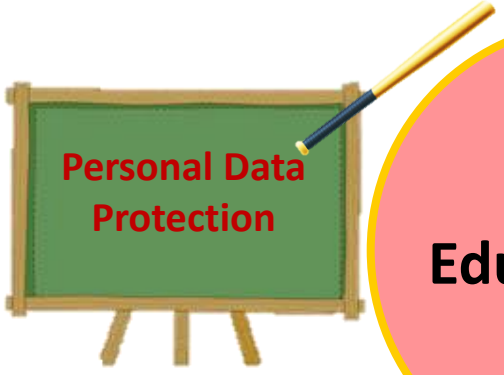
Hong Kong Association of Banks
Hong Kong Monetary Authority
1 April 2019

Use of Personal Data in the Digital Era

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

Role of PCPD

Enforcer



Educator

Facilitator

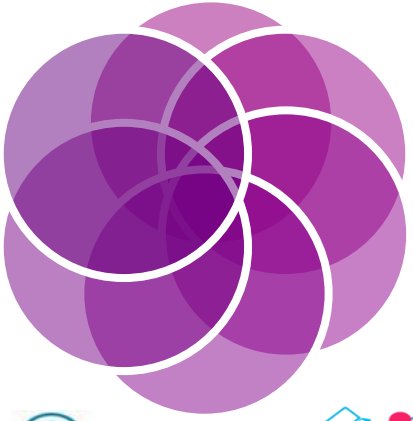
Proliferation of Fintech

Crowdfunding

E-wallet

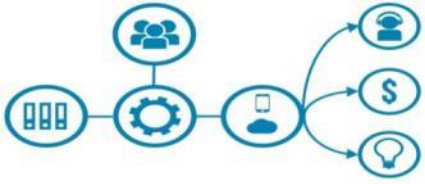
P2P Lending

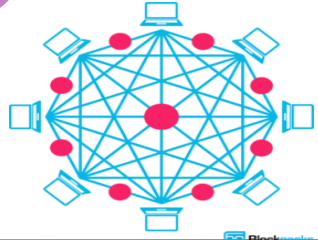
Robo-Adviser



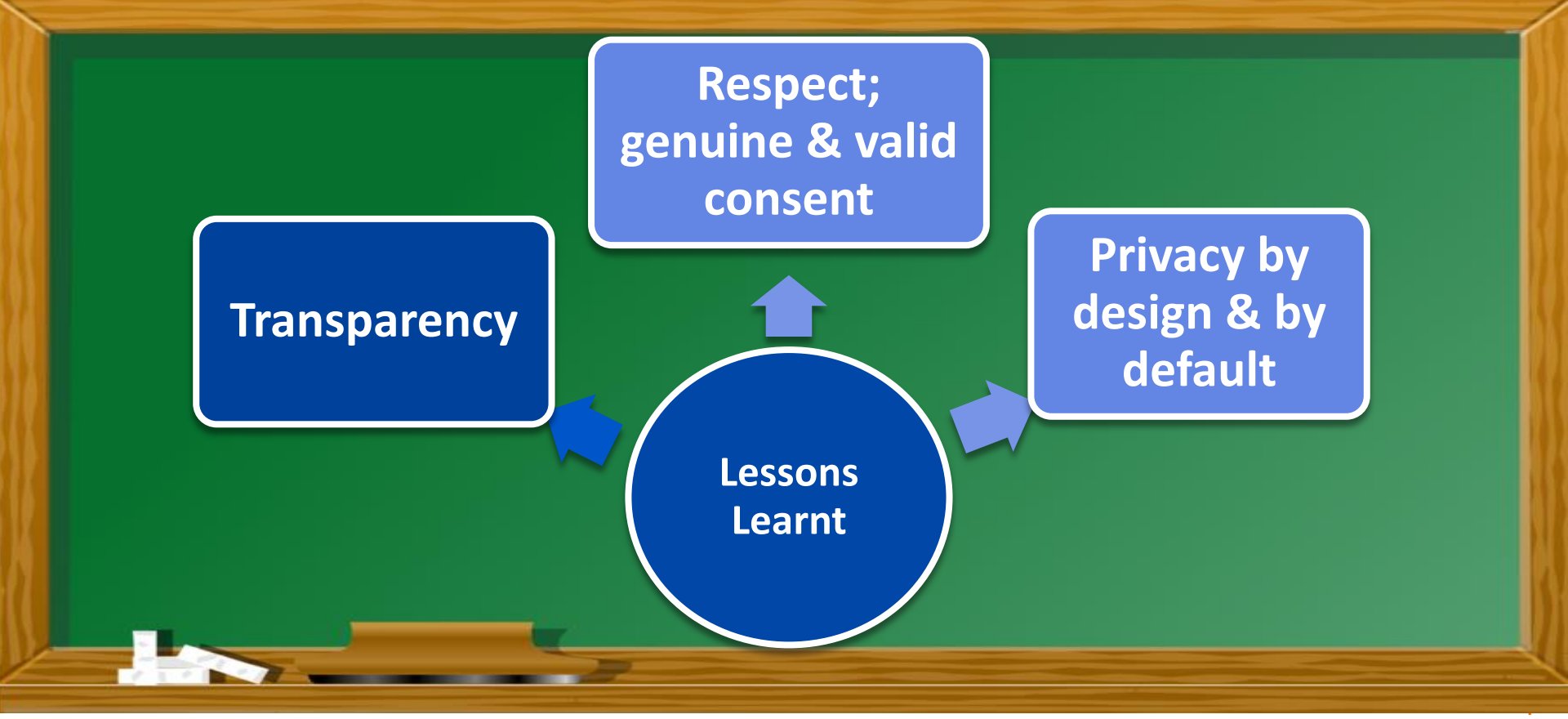
Credit Scoring

Open API



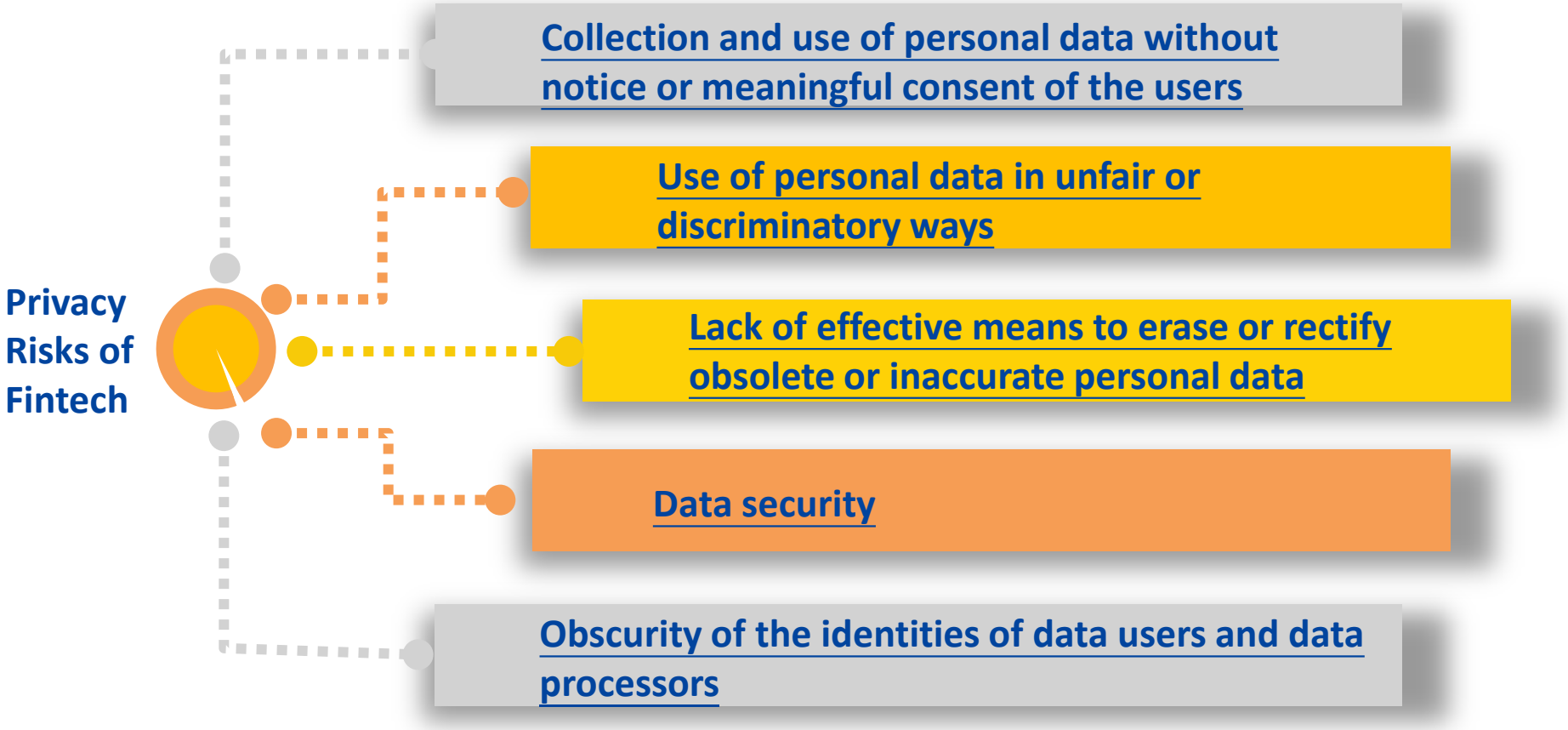


Blockchain


Respect; genuine & valid consent
Transparency
Privacy by design & by default
Lessons Learnt

Loophole of SMS-based 2-factor authentication

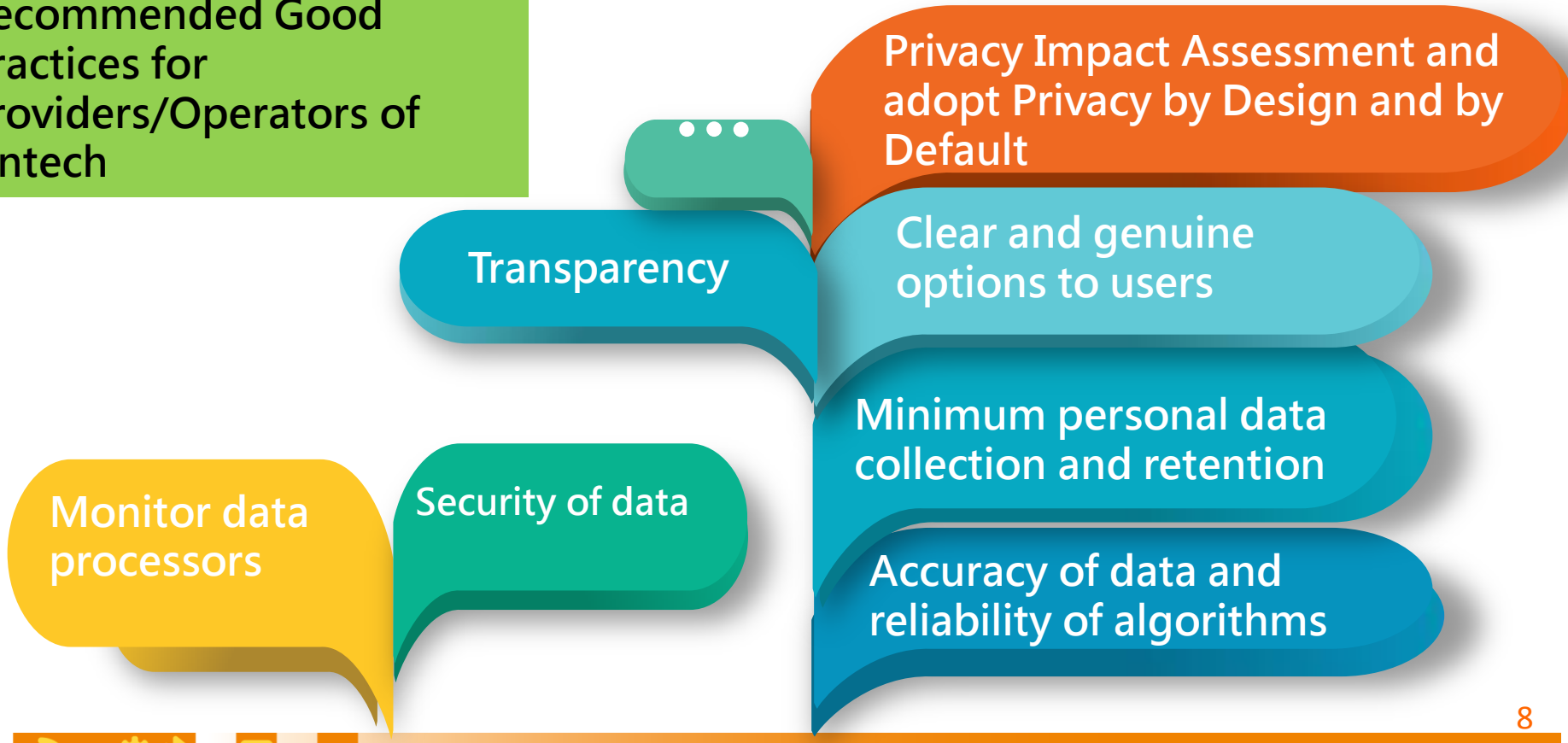
Sources: Apple Daily; Feb 2019


Privacy Risks of Fintech
Collection and use of personal data without notice or meaningful consent of the users
Use of personal data in unfair or discriminatory ways
Lack of effective means to erase or rectify obsolete or inaccurate personal data
Data security
Obscurity of the identities of data users and data processors

Vigilance for Users of Fintech

1. Carefully read the privacy policies
2. Operate the application softwares of Fintech under a safe environment
3. Critically assess requests for personal data and review privacy settings
4. Monitor account activities regularly

Recommended Good Practices for Providers/Operators of Fintech



Virtual Banking

Advantages	Challenges
Convenience : 7X24 cross-region and cross-border transactions	**Risk supervision**
Low Cost: • rent, renovation, wage →Higher deposit interest and Lower loan interest	**Customer protection**
Service Diversification: • innovative financial products and financial services • big data analysis and provide targeted services to customers	

Source: http://hd.stheadline.com/news/columns/792/20190308/746645/

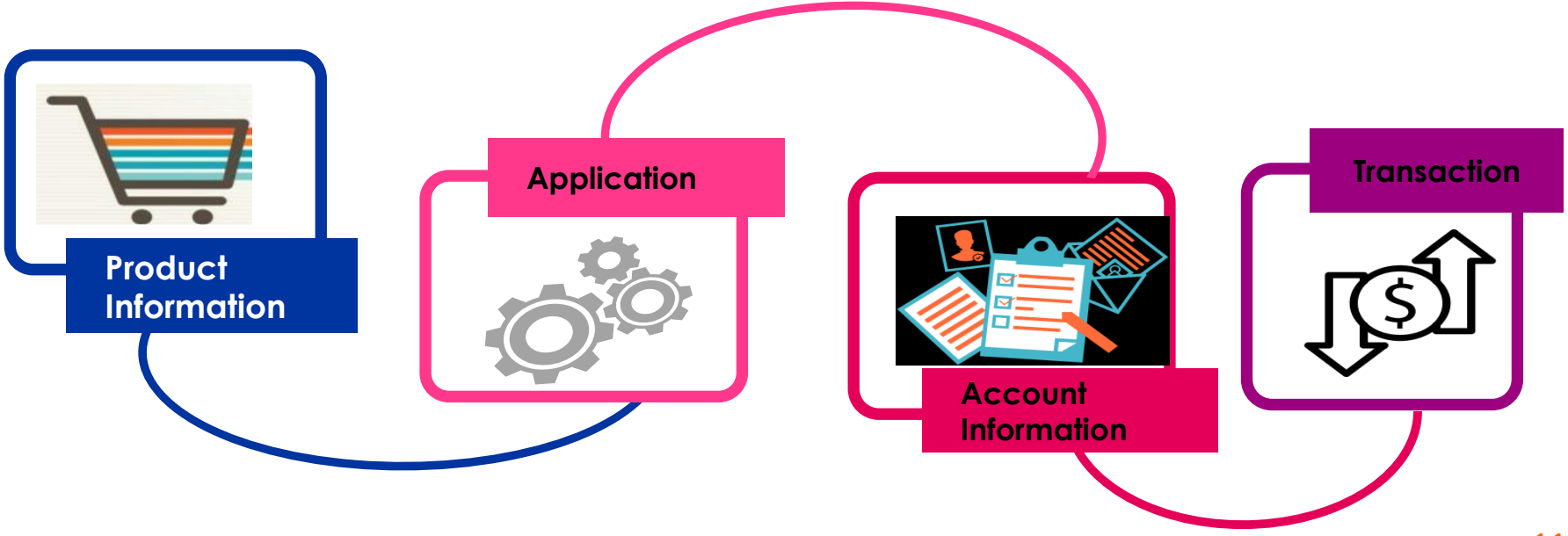
Privacy Risks of Virtual Banking

impersonation, identity theft, etc.

information security e.g. security breaches, hacking

collection of customers' information for profiling and analysis

Open API


Product Information
Application
Account Information
Transaction

Privacy Risks of Open API

- individuals may not have full understanding on the kinds of personal data that is shared with third-party developers and how the PD may be used and further disclosed
- service providers/operators may be inclined to collect and retain as much personal data as possible, even if the data may be inaccurate, irrelevant or obsolete
- transmitting personal data electronically among different organisations and end-users, which increases the risk of data leakage or interception during transmission
- individuals may not be able to ascertain who is liable for the leakage or mishandling of their personal data
- Customers may not be provided with clear and genuine options for the sharing of personal data

Information Leaflet on Fintech

New

- issued in March 2019
- privacy risks
- tips for users
- recommended good practices for providers/operators

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

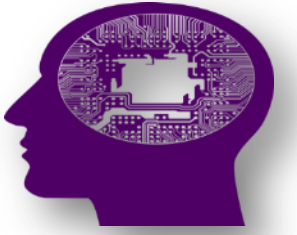

DATA

Data is the lifeblood of Fintech

1 **Collection of big data** (e.g., transaction records, behavioural data)

2 **Data analytics** (e.g., profiling, credit scoring)

3 **Automated decision making** (e.g., granting of loans, investment recommendations)



Privacy Challenges in Digital Economy

- Abuse of dominant position by "data monopolists"
- Lack of control and genuine choices by consumers

Competition

Privacy

- Excessive and covert data collection
- Exposure of sensitive information
- Unexpected, unfair and/or discriminatory use of data
- No meaningful consent

Data Security

- Hacking
- Data leakage

Cross-discipline and cross-border issues

- Consumer protection
- Cross-border data flow

The Digital Revolution

Ubiquitous collection of data

Unpredictability in use and transfer

Personal data belongs to the individuals

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

The Digital Revolution

Challenges for regulator:

- **To help facilitate the innovative use of data within the legal and ethical frameworks**
- **To help maximise the benefits of data in a sustainable way**
- **To minimise the risks of harm, creating healthy synergy with economic growth**

Reality (and danger) of the digital economy**:

- *Enterprises collect enormous amount of data from individuals*
- *Majority of the data is controlled by a small group of enterprises*
- *Ownership of data is not clear in laws*

**Chen Zhimin, former Vice-Minister, Ministry of Public Security

No matter…

Who should own your personal data?

… trust is indispensable.


Our customers' trust means everything to us. We spent decades working to earn that TRUST.
Tim Cook, 2015
Our data is being weaponised against us.
Tim Cook, 2018

“Trust is the new gold.”

Andrea Jelinek
Chair of European Data Protection Board

Least Common Multiple (LCM) approach: Accountability & Ethics

"Arguably the biggest change [brought by the GDPR] is around accountability."

Elizabeth Denham, Information Commissioner of the UK

"[The GDPR] aims to restore a sense of trust and control over what happens to our online lives."

Giovanni Buttarelli, European Data Protection Supervisor

Accountability and Governance

EU GDPR	HK PDPO
Risk-based approach to accountability. Data controllers are required to: • implement technical and organisational measures to ensure compliance [Art 24]; • adopt data protection by design and by default [Art 25]; • conduct data protection impact assessment for high-risk processing [Art 35]; and • (for certain types of organisations) designate Data Protection Officers [Art 37].	The accountability principle and the related privacy management tools are not explicitly stated. The Privacy Commissioner advocates the Privacy Management Programme which manifests the accountability principle. The appointment of data protection officers and the conduct of privacy impact assessment are recommended good practices for achieving accountability.

Data Ethics & Trust

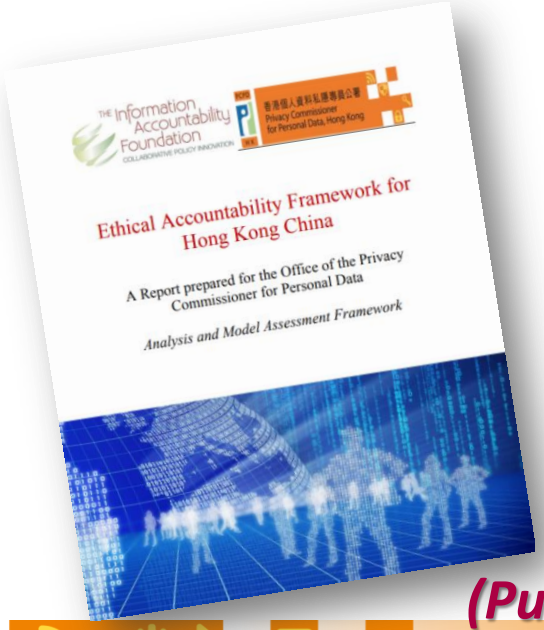
Ethics as a Bridge between Law and Expectation

- Business model and technological development vis-a-vis legislation and regulatory reform
- Public expectation forever increasing
- How to bridge the gap?
- Data Ethics

Ethics

“Ethical Accountability Framework for Hong Kong China”

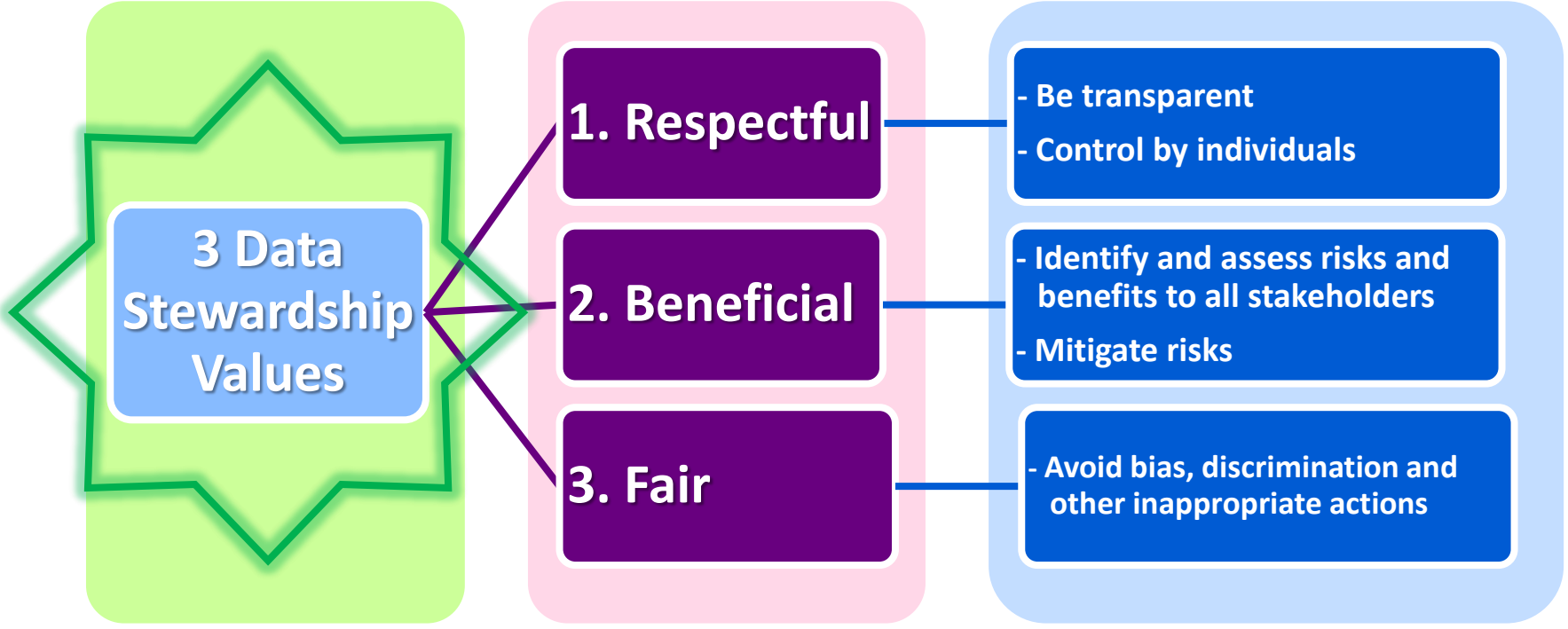
REPORT OF LEGITIMACY OF DATA PROCESSING PROJECT



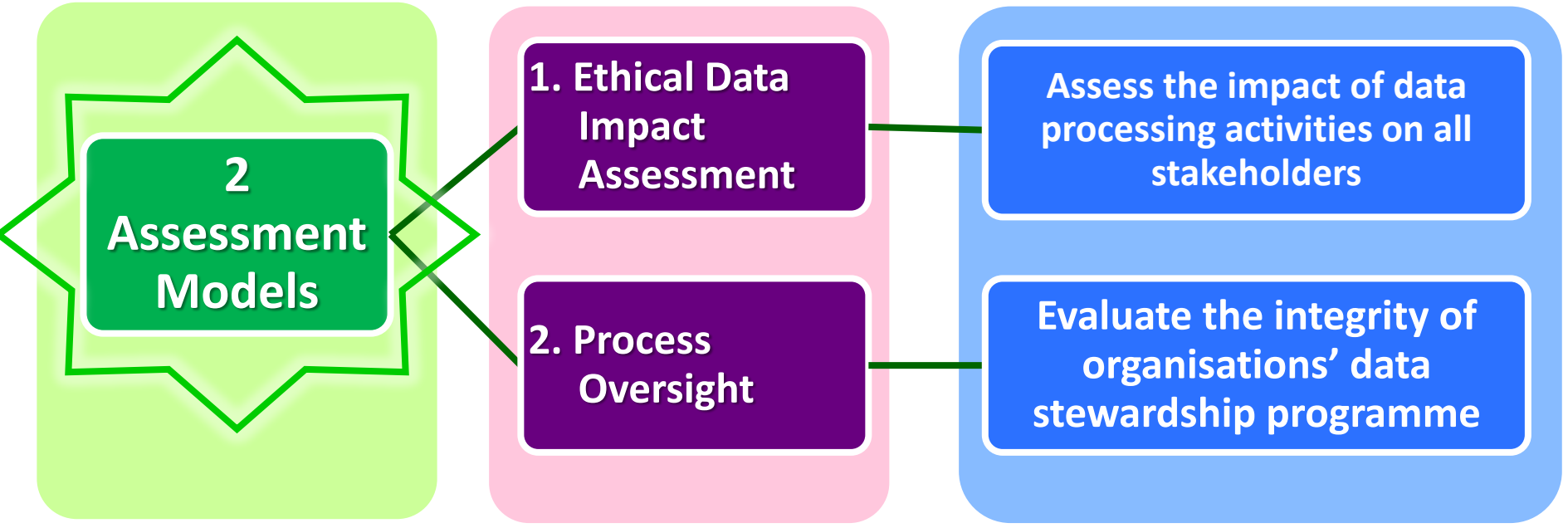
(Published on 24 October 2018)

Download >>

Multi-stakeholders' Approach – Three Core Values



Multi-stakeholders' Approach – Two Assessment Models

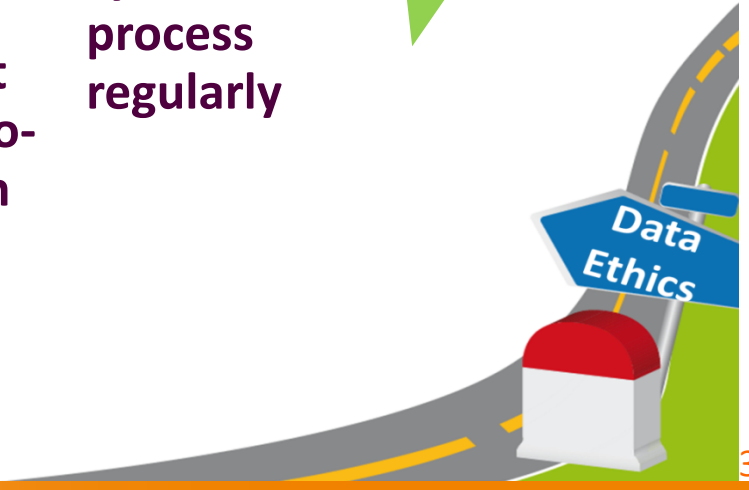


Data Ethics

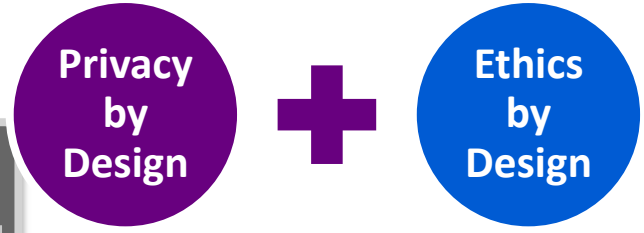
Think, plan and execute with multi-stakeholders' interests

Get data management on a cradle-to-grave basis in an institutional system and process

Review the system and process regularly



Data Ethics - Implementation



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

Examples of Privacy by Design and by Default

Under iOS 12.2, access to location data of iPhone or iPad by website operators is disabled by default

- To allow websites to their access location data, users have to switch on the function themselves, providing users with stronger control

Source: Ars Technica; Feb 2019

Examples of Privacy by Design and by Default

ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | Action we've taken

About the ICO / News and events / News and blogs /

ICO fines Uber £385,000 over data protection failings

Also paid $148 million in U.S.

Date 27 November 2018
Type News

The Information Commissioner's Office (ICO) has fined ride sharing company Uber £385,000 for failing to protect customers' personal information during a cyber attack.

A series of avoidable data security flaws allowed the personal details of around 2.7million UK customers to be accessed and downloaded by attackers from a cloud-based storage system operated by Uber's US parent company. This included full names, email addresses and phone numbers.

The records of almost 82,000 drivers based in the UK – which included details of journeys made and how much they were paid – were also taken during the incident in October and November 2016.

The ICO investigation found 'credential stuffing', a process by which compromised username and password pairs are injected into websites until they are matched to an existing account, was used to gain access to Uber's data storage.

- Uber changes its privacy settings after having been fined
  - ❖ 'hiding precise pickup and dropoff locations' in the driver app after a trip ends to help protect information about rider locations
  - ❖ riders and drivers can call or chat with each other directly in the Uber app, so rider no need to share their phone number

Source: ICO; Nov 2018

Examples of Ethics by Design

For personalised online advertising and marketing**:

- make it clear to the consumers if a recommendation of goods/services is a personalised advertisement; and
- provide consumers with information about other similar but non-personalised goods/services.

** Reference: draft revision to the Personal Information Security Specification of China (Jan-2019)

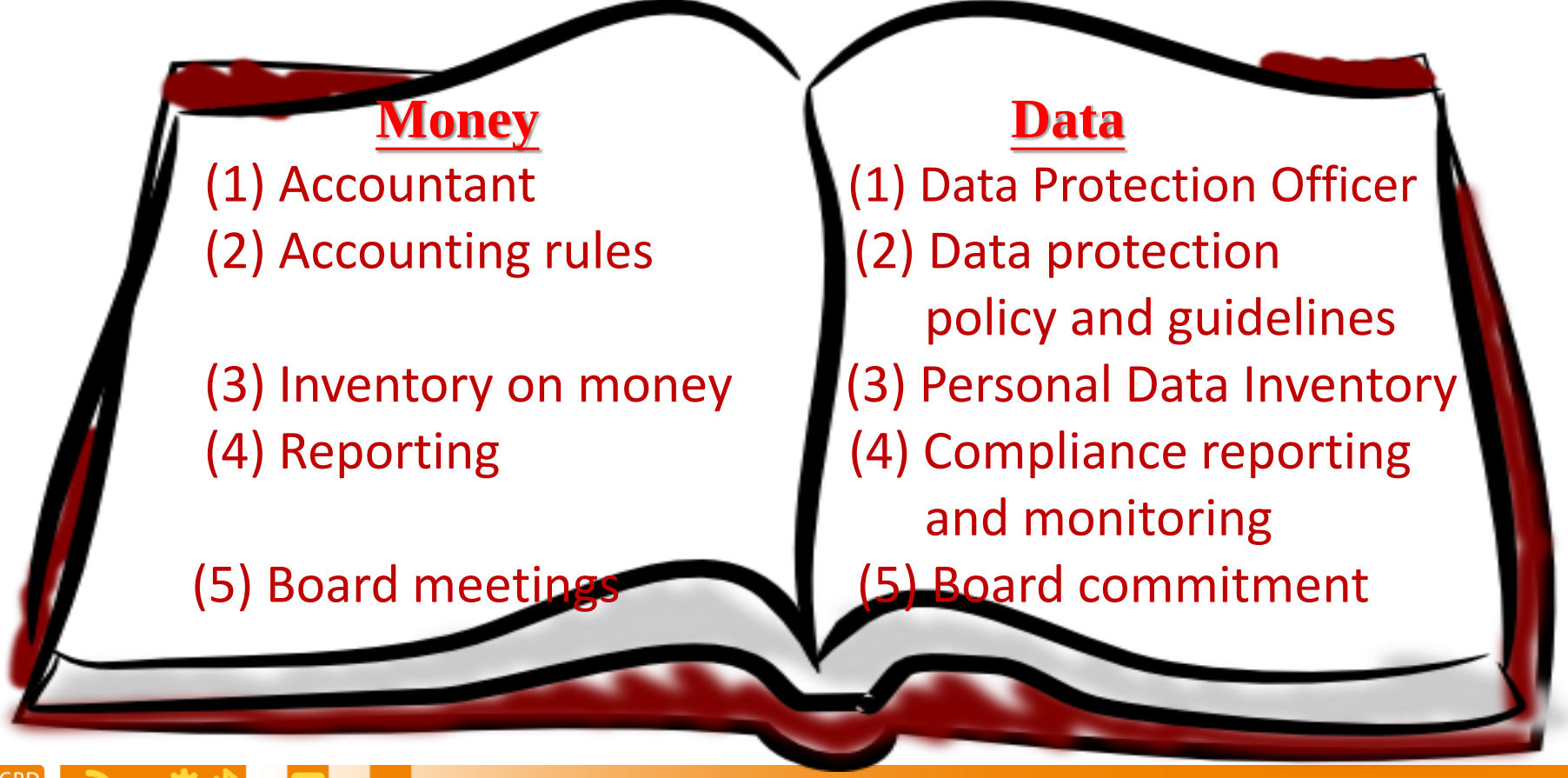
Data Governance & Accountability:

Privacy Management Programme (PMP)

Benefits

- Effective management of personal data
- Minimisation of privacy risks
- Effective handling of data breach incidents
- Demonstrate compliance and accountability

Treat Data as Money


Money
(1) Accountant
(2) Accounting rules
(3) Inventory on money
(4) Reporting
(5) Board meetings
Data
(1) Data Protection Officer
(2) Data protection policy and guidelines
(3) Personal Data Inventory
(4) Compliance reporting and monitoring
(5) Board commitment

PCPD's Roles – Enforcer + Educator + Facilitator

PCPD's Strategic Focus

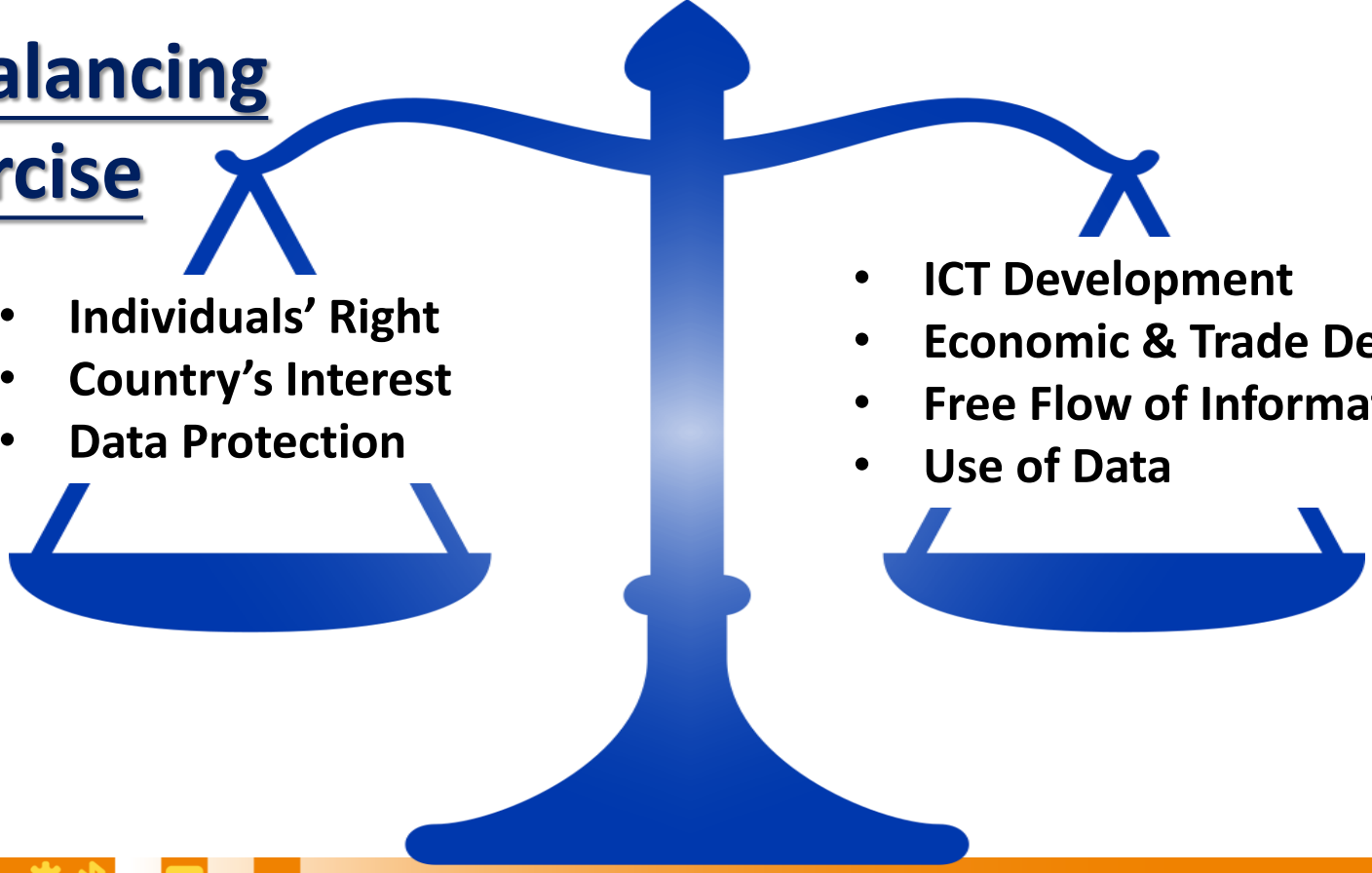
Fair Enforcement

Engaging

Incentivising

Privacy-friendly Culture

A Balancing Exercise

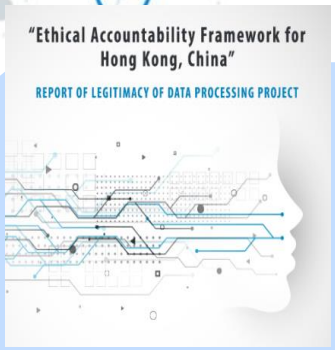


- Individuals' Right
- Country's Interest
- Data Protection

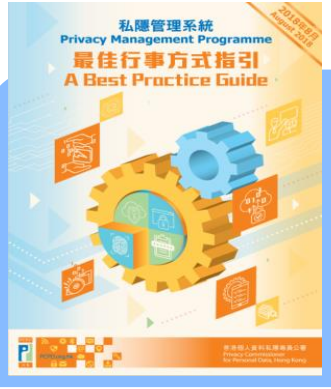
- ICT Development
- Economic & Trade Development
- Free Flow of Information
- Use of Data

Q&A

Thank you


"Ethical Accountability Framework for Hong Kong, China"
REPORT OF LEGITIMACY OF DATA PROCESSING PROJECT


Information Leaflet
Fintech
1. Introduction
2. Common Applications of Fintech


私隱管理系統
Privacy Management Programme
最佳行事方式指引
A Best Practice Guide


Legitimacy of Data Processing Project
Media Statement


European Union
General Data Protection Regulation
2016
(Effective 25 May 2018)

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