Seminar on Fintech
Application of Personal Data (Privacy) Ordinance and Best Practices for Fintech Firms

17 September 2019

Mr Tony Chik-ting LAM
Deputy Privacy Commissioner for Personal Data,
Hong Kong, China

Data is the lifeblood of the data-driven economy

1

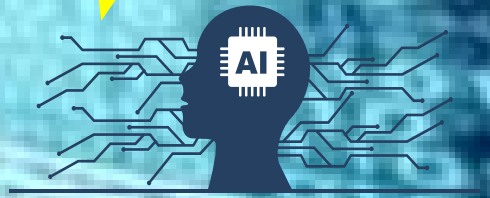
Collection of big data from various sources

2

Data analytics by AI

3

Automated decision making & improvement in business processes and services



Examples of Fintech

P2P Lending & Crowdfunding

E-wallet

Money transfer

Robo-Adviser

Financial planning

Credit Scoring

Hong Kong issues four more virtual bank licences to spur innovation and disrupt bricks-and-mortar financial services

- Four new licences granted, bringing the total to eight since March 2019
- The HKMA wants to spur innovation in financial services

Chad Bray
Enoch Yiu
Published: 6:33pm, 9 May, 2019

The exterior of the Hong Kong Monetary Authority (HKMA) on 27 October 2017. Photo: SCMP

Virtual Banking in Hong Kong

Source: https://www.scmp.com/business/article/3009574/hong-kong-issues-four-more-virtual-bank-licenses-spur-innovation-and

Examples of e-Wallet & Stored Value Facility (SVF)

- **Single Purpose SVF** – License not required, e.g. cake shop coupons
- **Device Based SVF**
  - Autotoll
  - Octopus
  - Unicard
- **Network based SVF**
  - WeChat Pay
  - Alipay
  - PayMe
  - O!epay
  - TNG

Underlying technologies of Fintech:

Artificial Intelligence

Blockchain

Cloud Computing

Big **D**ata

What about our Personal Data and Privacy?

Core Value

- Privacy as fundamental human right
- No absolute right
- Human dignity / humanity
- Balancing privacy rights and other human rights
- Not stifling ICT/ economic developments

Real and Normative Value

- **Ownership / control by individuals (EU GDPR)**
- **Expectation of individuals**

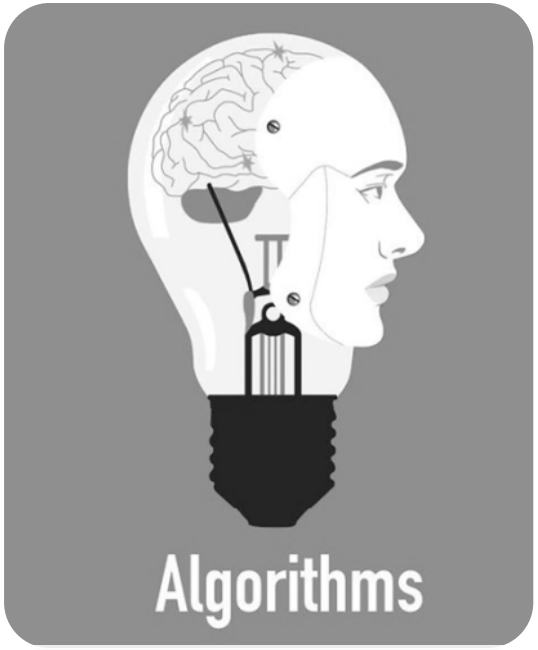
Six Data Protection Principles (DPPs) of the Ordinance

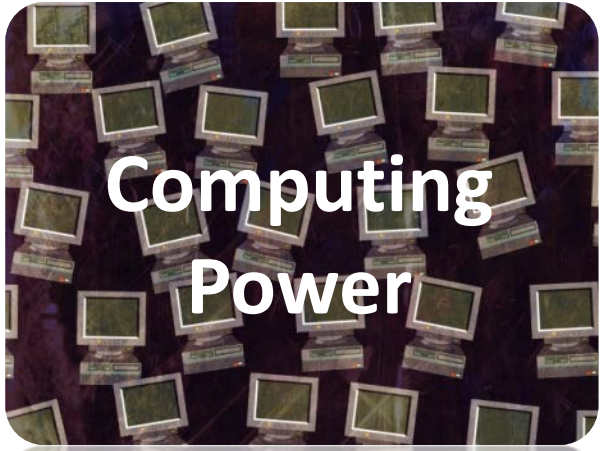
Animation of the six DPPs:
https://www.youtube.com/watch?v=j6fO6JVGGHg

Conflicts of technologies with Data Protection Principles

(1) Elements of AI in Fintech

e.g. Electronic payment history, location data, contact lists, electronic identification





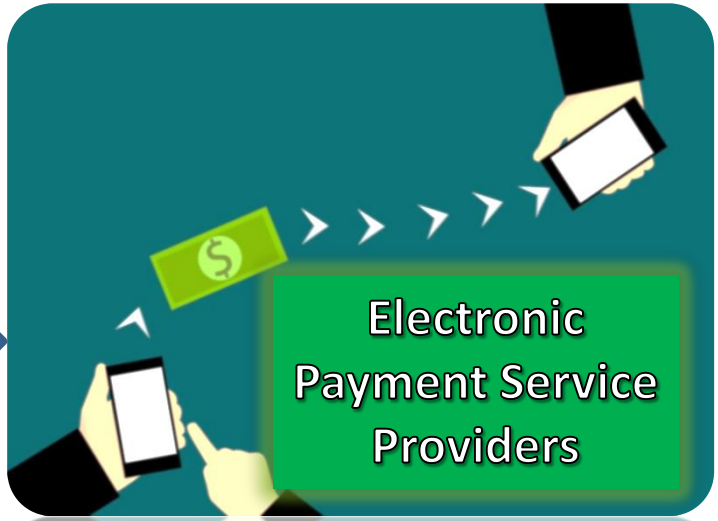
Big Data & AI in Fintech

Electronic Payment

Personal Data

AND Big Data

- Behavioural data (purchase history, preference)
- Location data
- Contact lists



Profiling

Big Data & AI in Fintech

HKMA 2018 Guideline

allows banks to use big data/consumer behaviour analytics to better manage credit risks

Analyse personal data to determine credit

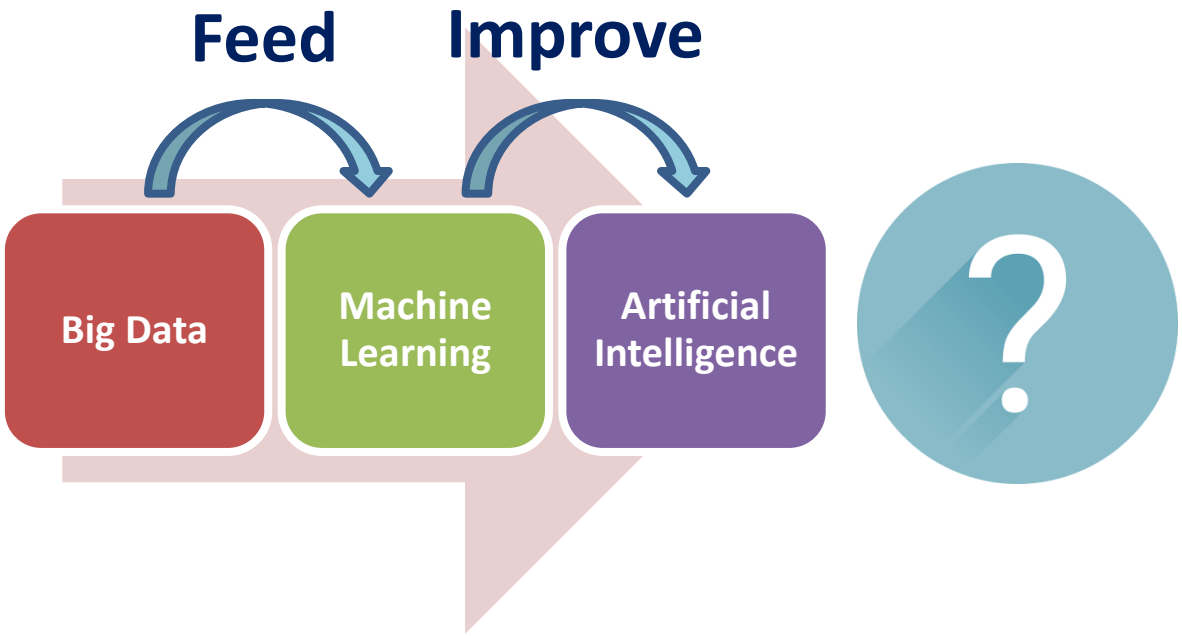
e.g. purchase history, payment records, neighbourhood, social network and other behavioural data

Hang Seng Bank to relax loans rules, using big data and fintech to replace old-fashioned banking

Enoch Yiu
Published: 7:26pm, 28 Jun, 2018

Source: https://www.scmp.com/business/banking-finance/article/2152968/hang-seng-bank-relax-loans-rules-using-big-data-and-fintech

Risks of AI & Big Data



- Excessive collection
- Lack of transparency
- Unpredictable use
- Bias & discrimination resulting from inaccurate predictions
- Loss of control by individuals
- Manipulate human behaviour

Excessive collection → Privacy intrusive?

Lack of transparency → Meaningful consent?

Unpredictability → Acceptable / allowable use?

Bias and discrimination → Fair?

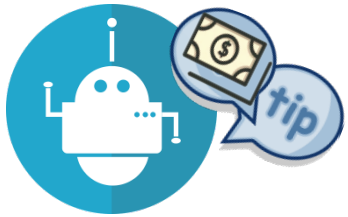
Manipulation & Loss of control → Freedom & dignity?

Example of unfair predictive credit scoring

US Federal Trade Commission (FTC) report – *Big Data* (2016):

- Banks assessed credit risks of customers based on their shopping histories
- All customers of a certain store were given lower credit scores because many customers of the store did not repay on time
- Customers were in dark about the bank's scoring algorithms
- Lower credit score was not fair to some customers who repaid on time

Example: Securities and Futures Commission (SFC) Guidelines for Robo-advice



- "Guidelines on Online Distribution and Advisory Platforms" by SFC, July 2019
- Applies to:
  - Provision of financial advice in an online environment using algorithms and other technology tools
  - Uses of data and algorithms to profile clients and devise responses
- Requirements:
  - Information about the algorithm and its limitations must be provided to clients
  - Internal controls in place to supervise algorithm, prevent unauthorised access

(2) Three Main Types of Blockchains

Public Blockchain

Basic type: accessible to anyone anywhere

Anyone can record transaction, validation, get a copy of data

Permissioned Blockchain

Similar to public blockchain; only with rules on top about who is allowed to take part in what

"Private" Blockchain

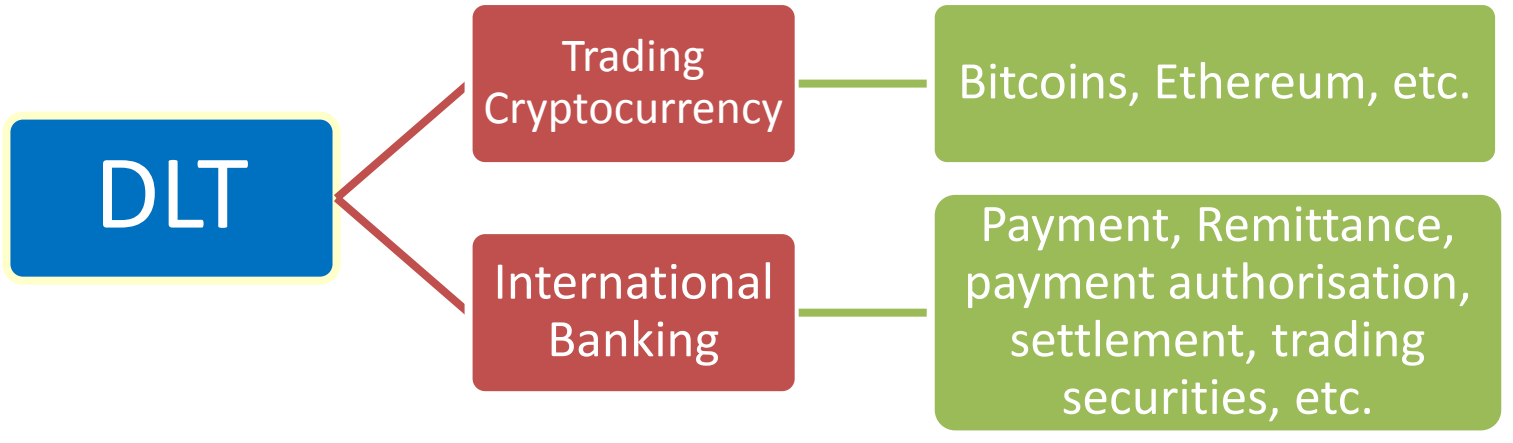
Controlled by a central unit overseeing data and validation

Not seen by "proper" blockchains by some

Privacy Risk INCREASES

Blockchain in Fintech

Distributed Ledger Technology (DLT)



Four characteristics of Blockchains

Sharing/ Decentralization

(Data can be viewed by all)

Limited Access Control

(Data can be viewed by all)

Irreversibility

(No amendment or deletion)

Disintermediation

(Who is data user?)

Seem to go against many data protection principles

CNIL (French Data Protection Authority)

Guidance on Blockchain Use (2018)

- Organisations should carefully exercise caution in deciding if they need to use blockchains, especially if a public one
- Data minimization should be prioritized --- in response to the fact that they cannot be deleted once on there
- Possibly recognizes all participants in blockchain as “data controllers”

(3) Cloud Computing in Fintech

'Cloud First Strategy'

- HSBC migrated data partially to Google Cloud Platform (GCP), to use Google's big data, analytics and machine learning capabilities
- Darryl West, group chief information officer at HSBC: *"Access to Google Cloud technology will help us to offer our customers the banking services they want and expect, to safeguard their data and their finances, and to run our business more efficiently."*

Source: https://www.fintechfutures.com/2018/07/hsbc-boosting-cloud-capabilities-with-google/ ; https://www.silicon.co.uk/cloud/hsbc-google-cloud-211037

HSBC Embraces Google Cloud For Big Data Analytics And Money Laundering Detection

Roland Moore-Colyer, May 4, 2017, 1:03 pm

BIG DATA | BUSINESS INTELLIGENCE | CLOUD | CLOUD MANAGEMENT | DATA STORAGE | DATABASE | IAAS | WORKSPACE

Privacy Risks of Cloud Computing

- Rapid cross-border/boundary data flow
- Unknown/little control over data storage locations
- Rapidly changing/Loose outsourcing arrangements
- Standardised contracts adopted by the cloud service providers – no tailored service

Problematic for:
Data Retention
Data Security
Cross-border transfer

Cloud Computing and Personal Data Privacy

Bottom Lines

Hong Kong - Cross-border/boundary transfer of Personal Data

- **Section 33 of the PDPO**
  - Regulates Cross-border Data Transfer
  - This section is **not yet in force**
  - General prohibition of Cross-border Data Transfer UNLESS one of the conditions specified under section 33(2) is satisfied

Section 33 of PDPO

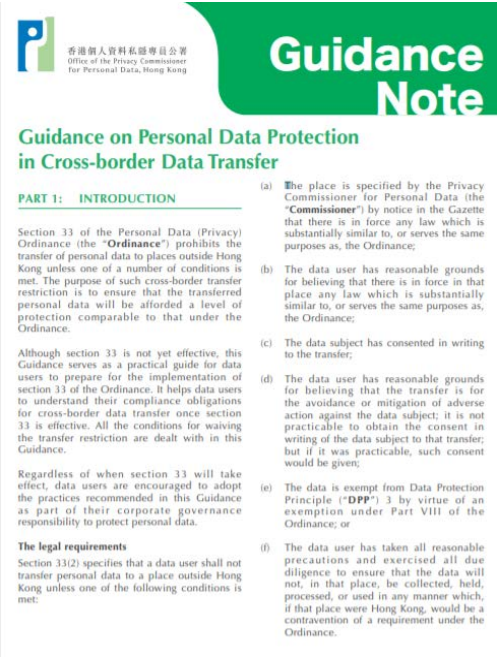
Transfer of personal data outside HK is prohibited **except** under any one of the following specified circumstances:-

1. Transfer to places specified in "White List"
2. Adequate data protection regime in the destined jurisdiction
3. Written consent by data subjects
4. Transfer for avoidance and mitigation of adverse action against data subjects
5. Use of personal data is exempted from DPP3
6. Reasonable precautions and due diligence taken by data users

Hong Kong - Cross-border / boundary Transfer of Personal Data

- PCPD issued Guidance Note on Personal Data Protection in Cross-border Data Transfer (2014)

- Model contract clauses for cross-border/boundary transfer



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

Guidance Note

Guidance on Personal Data Protection in Cross-border Data Transfer

PART 1: INTRODUCTION

Section 33 of the Personal Data (Privacy) Ordinance (the "**Ordinance**") prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. The purpose of such cross-border transfer restriction is to ensure that the transferred personal data will be afforded a level of protection comparable to that under the Ordinance.

Although section 33 is not yet effective, this Guidance serves as a practical guide for data users to prepare for the implementation of section 33 of the Ordinance. It helps data users to understand their compliance obligations for cross-border data transfer once section 33 is effective. All the conditions for waiving the transfer restriction are dealt with in this Guidance.

Regardless of when section 33 will take effect, data users are encouraged to adopt the practices recommended in this Guidance as part of their corporate governance responsibility to protect personal data.

The legal requirements

Section 33(2) specifies that a data user shall not transfer personal data to a place outside Hong Kong unless one of the following conditions is met:

(a) The place is specified by the Privacy Commissioner for Personal Data (the "**Commissioner**") by notice in the Gazette that there is in force any law which is substantially similar to, or serves the same purposes as, the Ordinance;

(b) The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance;

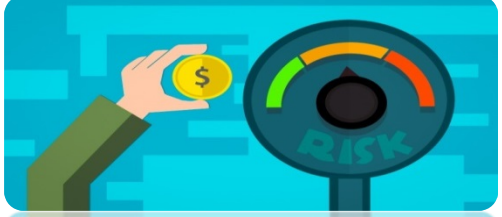
(c) The data subject has consented in writing to the transfer;

(d) The data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given;

(e) The data is exempt from Data Protection Principle ("**DPP**") 3 by virtue of an exemption under Part VIII of the Ordinance; or

(f) The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed, or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance.

Data-related Risks to Business



- Customer Defection
- Financial Loss
- Enhanced Regulatory Enforcement
- Operations Disruption

(1) Customer Defection

Data Breach,

Privacy Scandals

Customers' trust impaired

Customer Defection

A 2019 survey by Microsoft shows, in an event of a privacy or security breach…

- **53%** of consumers in the Asia Pacific region would…
  - **Switch** to another organisation,
  - **Reduce** the usage of the digital service, or
  - **Stop** using the digital service altogether

(2) Financial Loss

In 2018, Facebook's share price…

- **Dropped 6%** - After the Cambridge Analytica incident
- **Dropped 19%** - After quarterly report showed 3 million European users left due to the Cambridge Analytica incident

(3) Enhanced Regulatory Enforcement

Hefty monetary fines could be imposed for mishandling data

EQUIFAX

- Credit data leakage in 2017 affected **147 million consumers**
- **$575 million** for settlement with the Federal Trade Commission, Consumer Financial Protection Bureau, and US states

(4) Operations Disruption

Ransomware

Cyberattack (e.g. DDoS)

Poor Data Governance

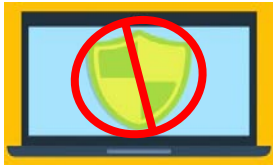
+

Inadequate Data Security

→

Disruption in Operations

Harm Sustainability of Operations

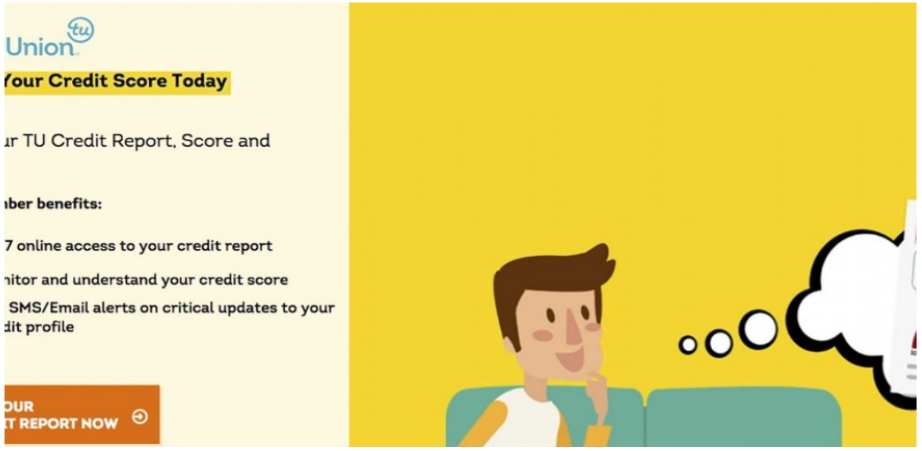


Hong Kong economy

Credit reporting agency TransUnion forced to suspend online services over personal data security flaw as Hong Kong leader urges fix

- Chief Executive Carrie Lam was among those affected by easy online authentication procedures
- TransUnion, which compiles credit reports for banks and lending institutions, handles the data of 5.4 million consumers in Hong Kong

Denise Tsang
Published: 7:15pm, 29 Nov, 2018



Source: https://www.scmp.com/news/hong-kong/hong-kong-economy/article/2175654/credit-agency-transunion-suspends-online-services

Data Security Incident - TransUnion

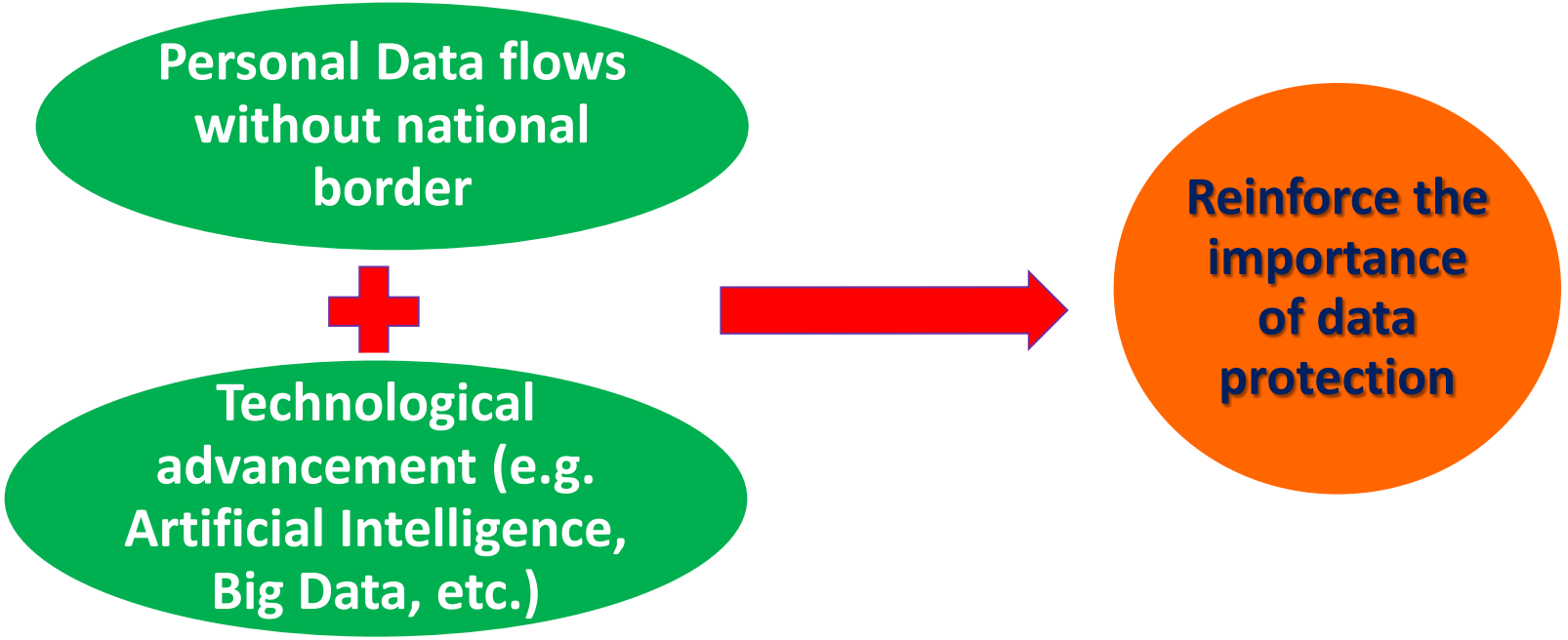
Microsoft – IDC Study: Only 31% of consumers In Asia Pacific trust organizations offering digital services to protect their personal data

April 16, 2019 | Microsoft Asia News Center

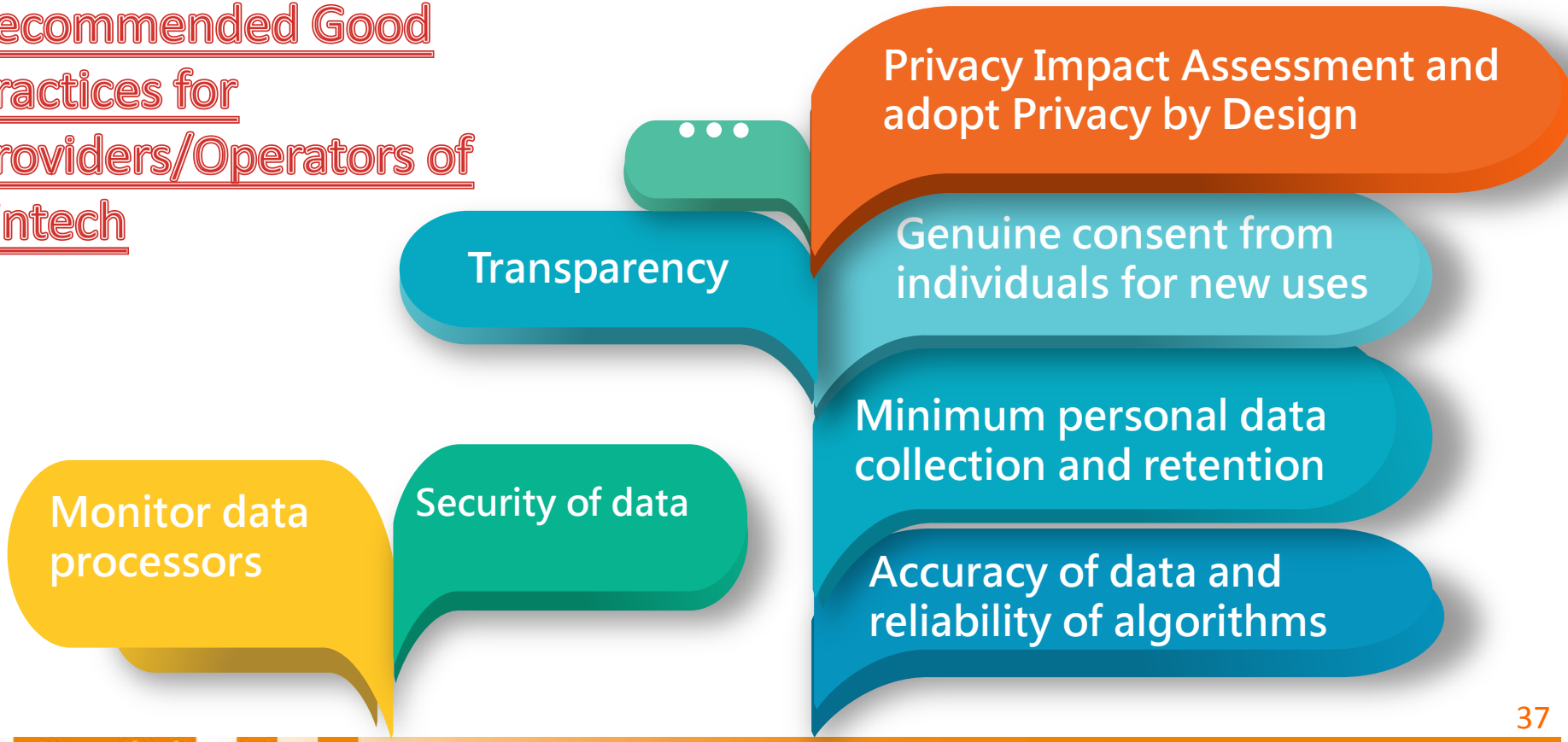
- **Only 31% of consumers trust organisations offering digital services to protect their personal data**
- **More than 50% of consumers will switch to another organisation in the event of negative trust experience, such as breach of security and privacy**

Source: Microsoft (April 2019)
https://news.microsoft.com/apac/2019/04/16/microsoft-idc-study-only-31-of-consumers-in-asia-pacific-trust-organizations-offering-digital-services-to-protect-their-personal-data/

Role of Hong Kong as the regional data/innovation hub



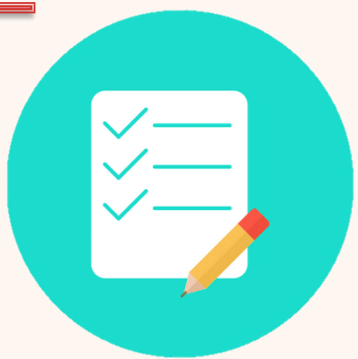
Recommended Good Practices for Providers/Operators of Fintech



Tips 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

General Recommended Principles



1. Accountability
2. Data Ethics
3. Return of control to individuals
4. Data security – all practicable steps

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

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

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

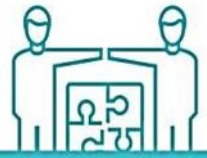
PCPD's Accountability Framework:

Privacy Management Programme (PMP)

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

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

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

2.1
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

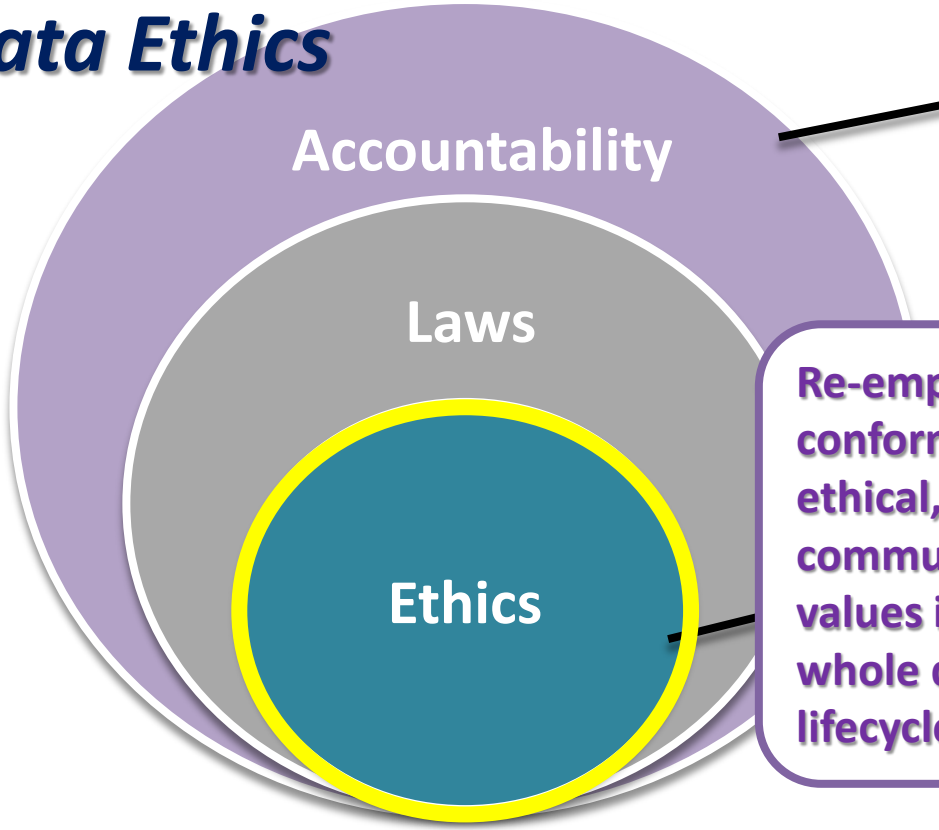
3.2
Assessment & Revision of Programme Controls

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



Extended obligation to ensure compliance with laws

Legal obligations, usually based on communal values

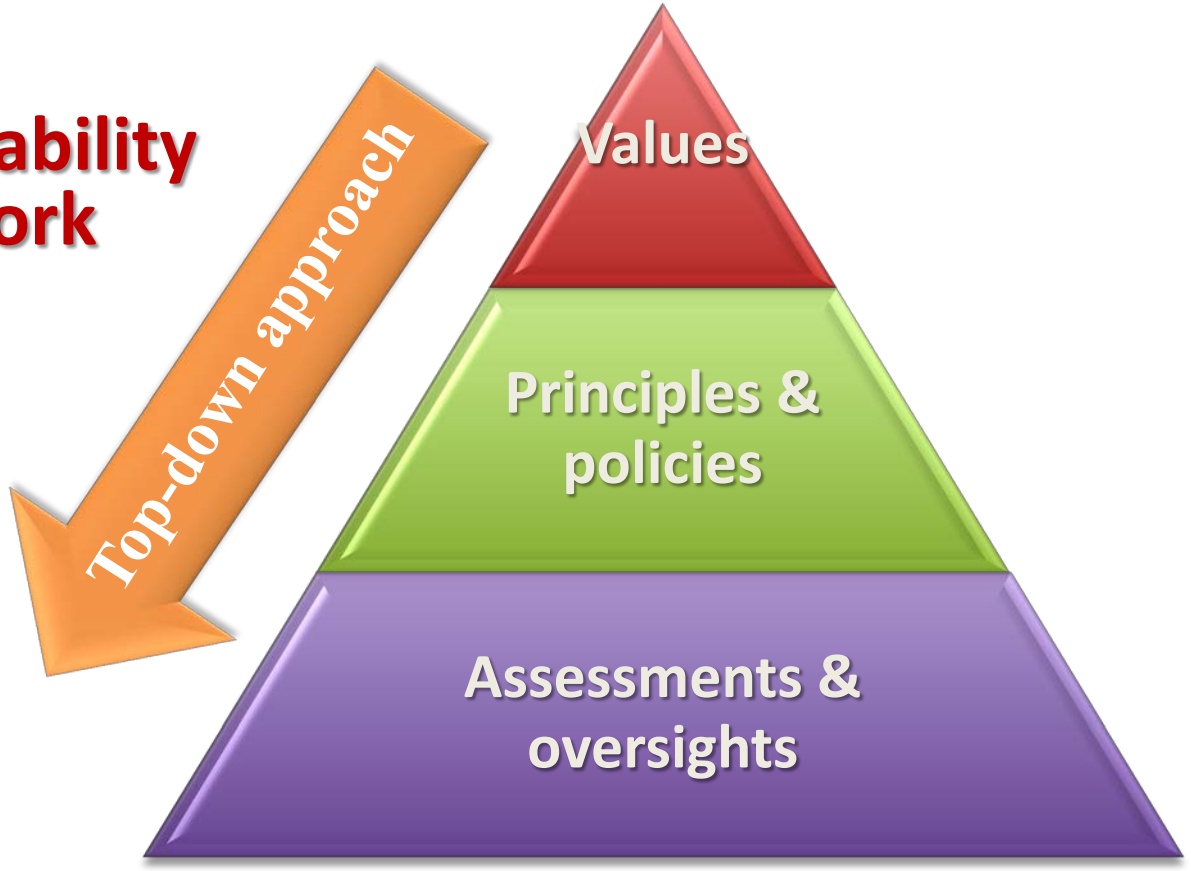
Communal values shared by the public in general, guiding our daily living

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

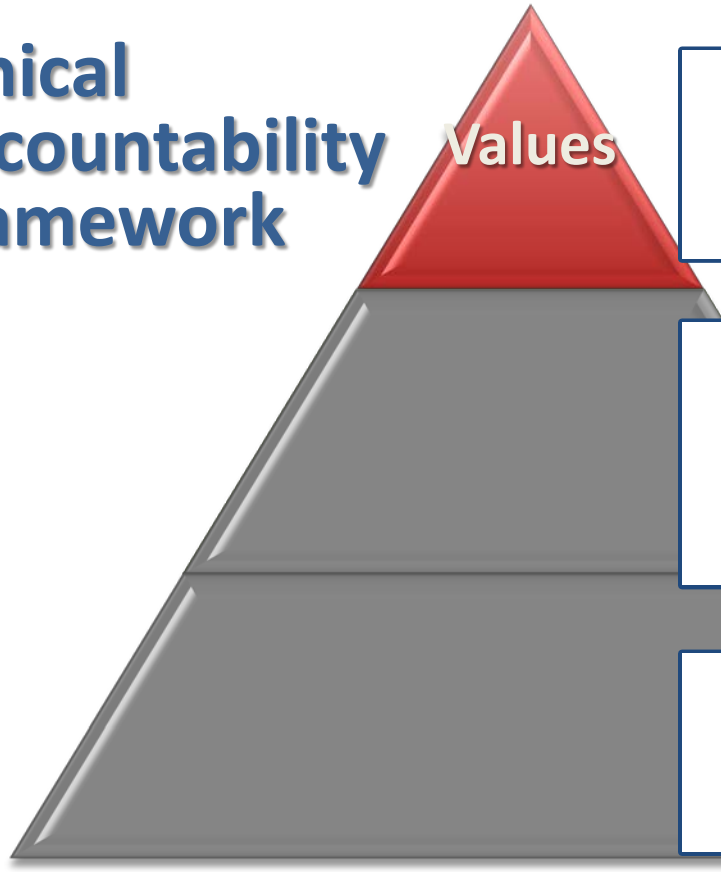
Ethics as a Bridge between Law and Expectation

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

Ethical Accountability Framework



Ethical Accountability Framework



1. Respectful

- Be transparent
- Provide individuals with control

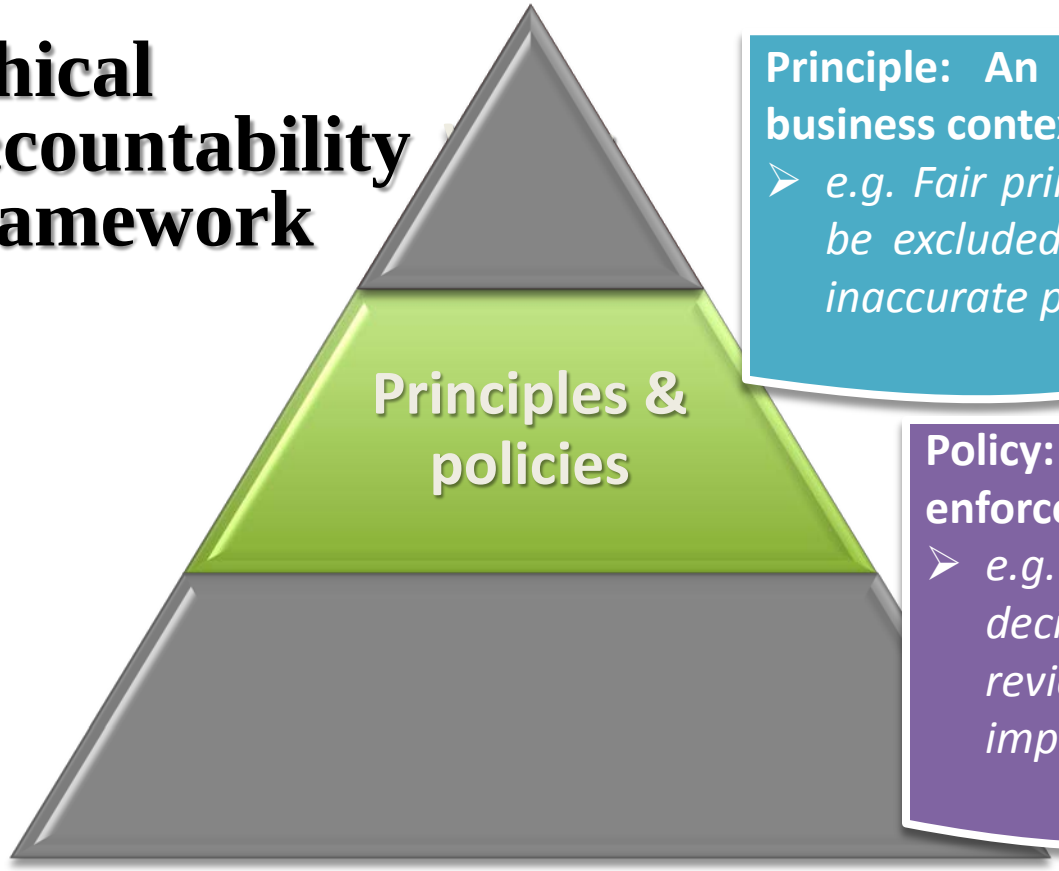
2. Beneficial

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

3. Fair

- Avoid bias, discrimination and other inappropriate actions

Ethical Accountability Framework



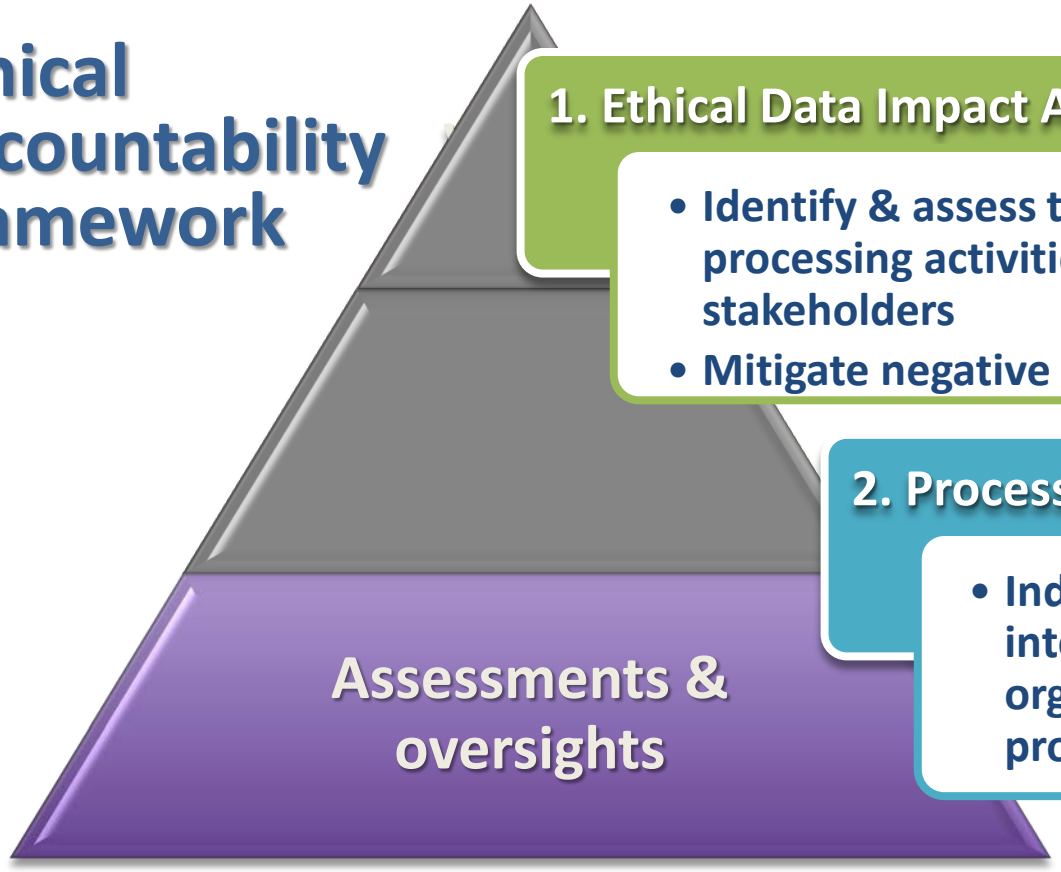
Principle: An expression of Values in business context

- *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 & Trust

Consumers

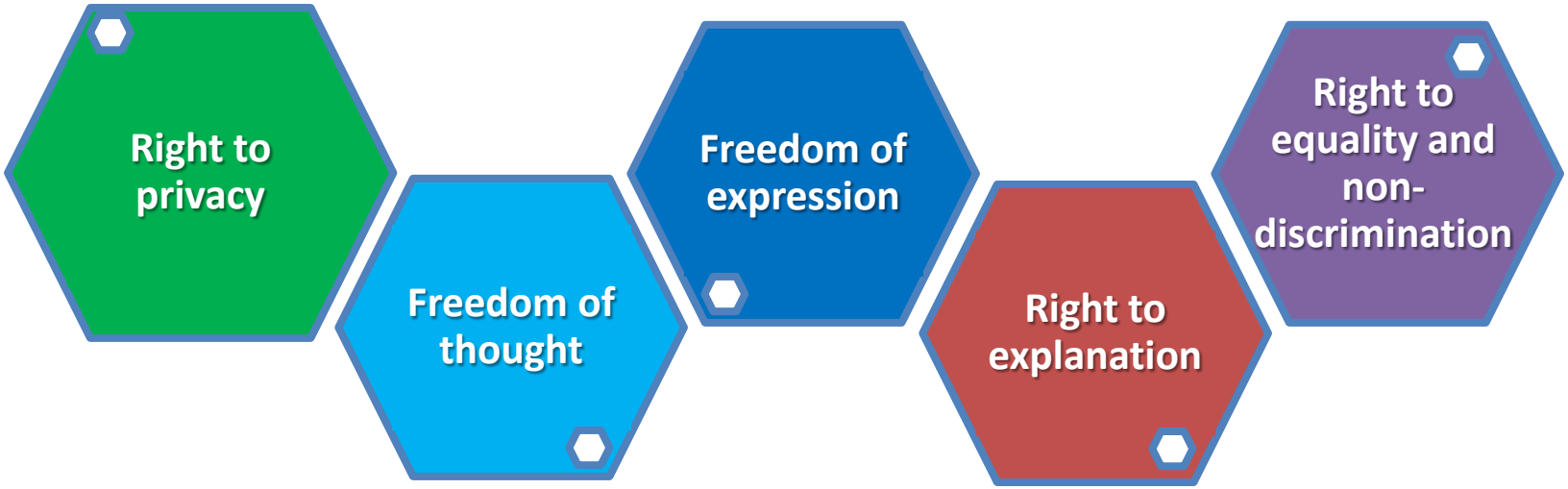
Data

Profiling or credit scoring, facilitating automated decisions → Grant loans, recommend investment…

Businesses

Ethical Obligations

Rights and interests of Data subjects:



…return control to individuals.

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


Declaration on Ethics and Data Protection in Artificial Intelligence

ICDPPC
International Conference of Data Protection & Privacy Commissioners

DECLARATION ON ETHICS AND DATA PROTECTION IN ARTIFICIAL INTELLIGENCE
40th International Conference of Data Protection and Privacy Commissioners
Tuesday 23rd October 2018, Brussels

AUTHORS:
- Commission Nationale de l'Informatique et des Libertés (CNIL), France
- European Data Protection Supervisor (EDPS), European Union
- Garante per la protezione dei dati personali, Italy

CO-SPONSORS:
- Agencia de Acceso a la Información Pública, Argentina
- Commission d'accès à l'information, Québec, Canada
- Datatilsynet (Data Inspectorate), Norway
- Information Commissioner's Office (ICO), United Kingdom
- Préposé fédéral à la protection des données et à la transparence, Switzerland
- Privacy Commissioner for Personal Data, Hong Kong
- Data protection Authority, Belgium
- Data protection Commission, Ireland
- Data Protection Office, Poland
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), Mexico
- National Authority for Data Protection and Freedom of Information, Hungary
- Federal Commissioner for Data Protection and Freedom of Information, Germany
- Office of the Privacy Commissioner (OPC), Canada
- National Privacy Commission, Philippines

1 | Page

Fairness principle

Reducing biases or discriminations

Continued attention and vigilance

Empowerment of every individual

Systems transparency and intelligibility

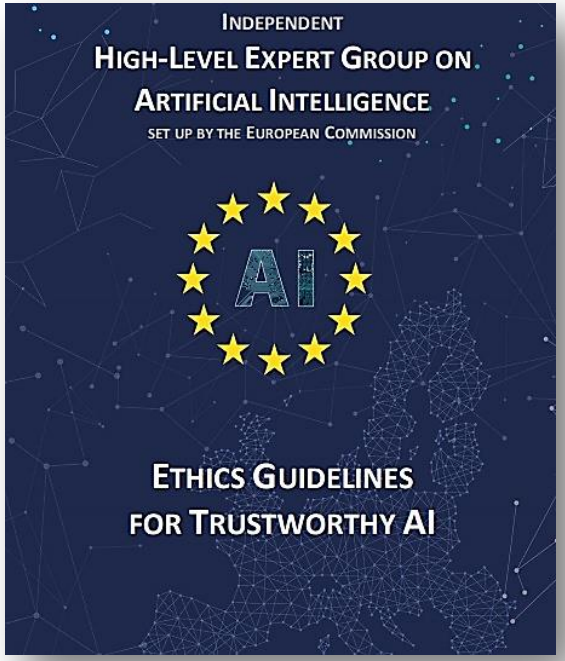
Ethics by design

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

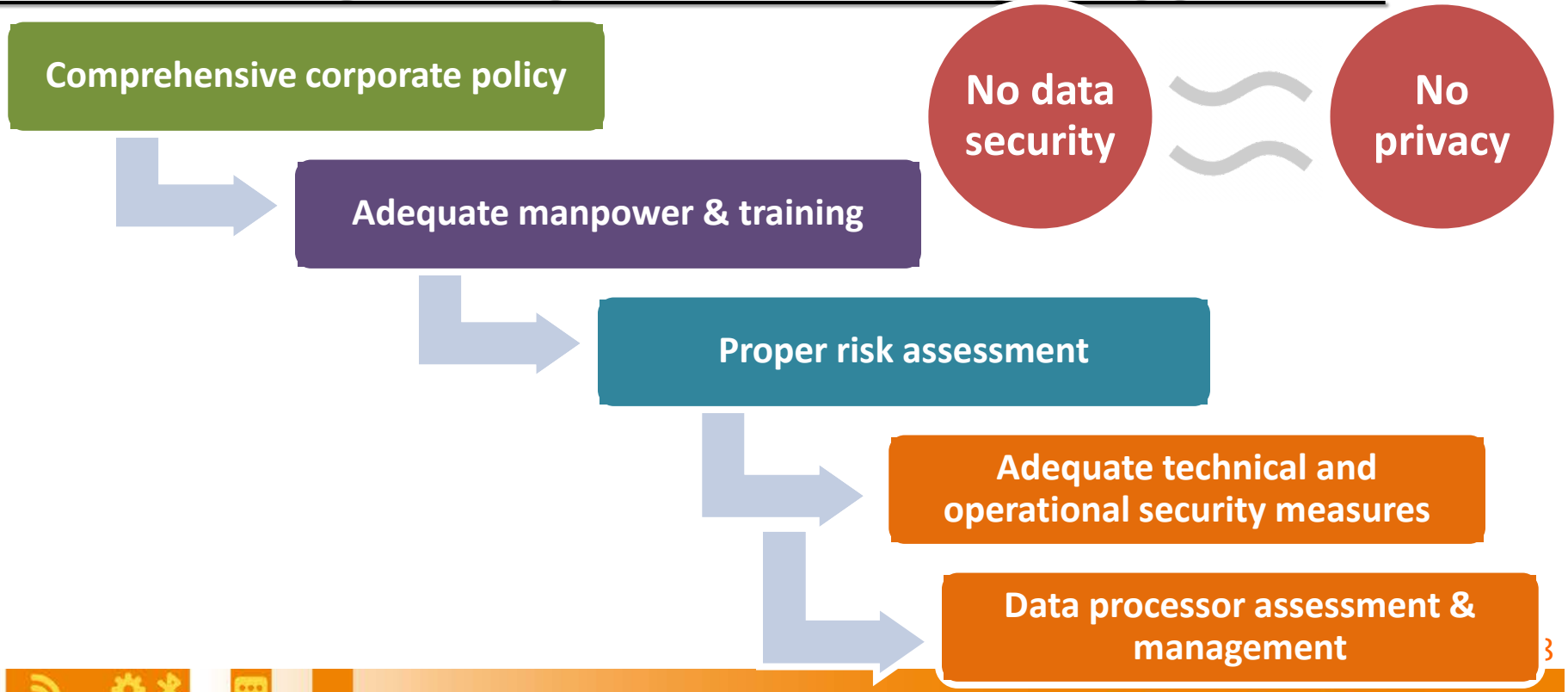
EU's "Ethics Guidelines for Trustworthy AI" (2019)



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

Data security – *'All practicable steps' approach*



Data Security: Adoption of Cybersecurity Risk Management

e.g. NIST's Risk Management Framework

Preparation

Essential preparations, categorisation and selection for managing data security risks

e.g. assign key roles, identify key processes, determine adverse impact of incidents, select and tailor controls necessary

Implementation

Implement controls in the security plans

Assess if the implementation are effective for the desired outcomes

Monitoring

Provide **organisational accountability** by senior management assessing if risks are properly addressed

Maintain **continuous monitoring** and situational awareness

Data Processor Management –

How should financial institutions manage Cloud Service Providers?

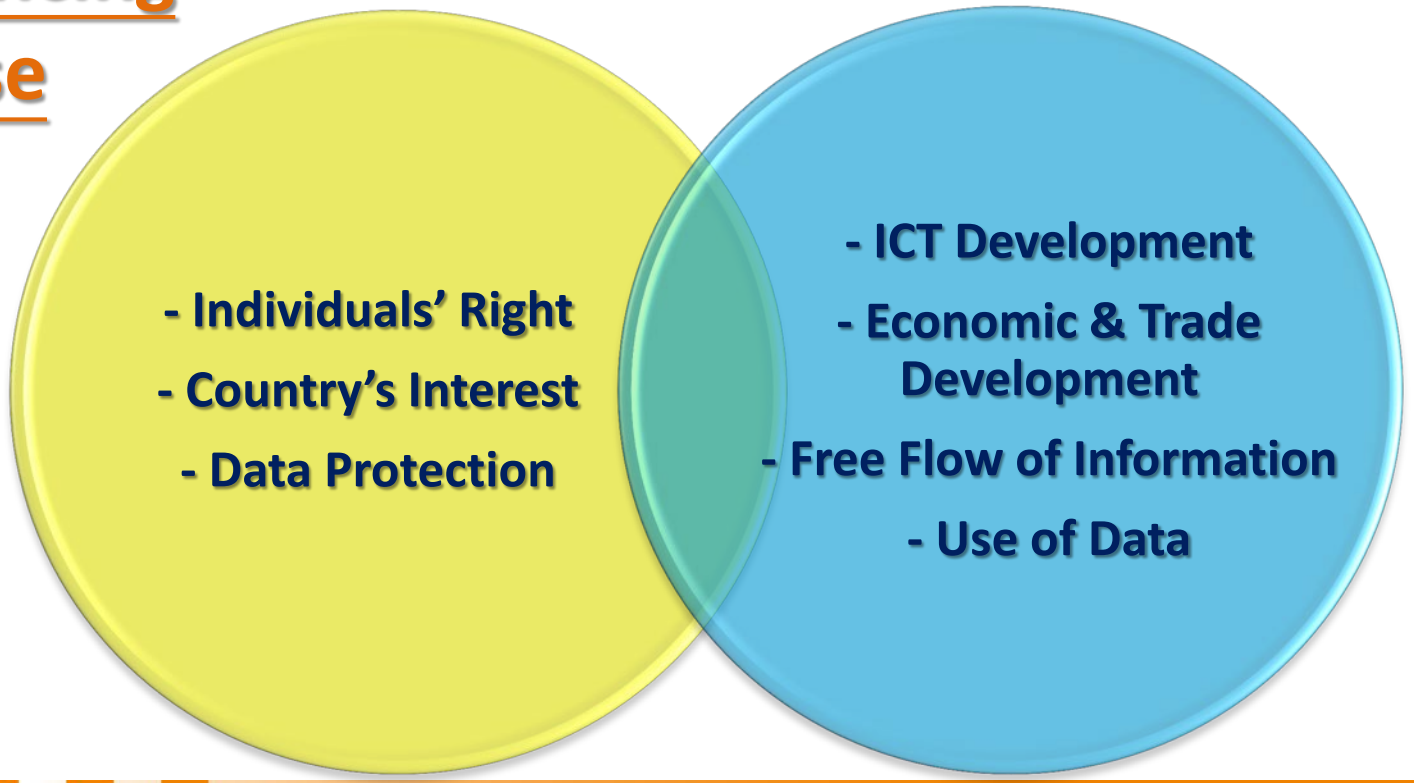
Data users are legally responsible for the actions of their agents; they should make certain:

- Adequate and effective **protection** of personal data, e.g. encryption of data in transit and in storage
- Clear **notification to customers** about the outsourcing to cloud service providers

Ensure the service contract has the provisions to:

- Limit the **use** of personal data to the specific purpose only
- **Erasure or return** of data to data user upon request
- Allows for customers to **access**, **correct**, and **resolve issues/ complaints** about their personal data
- Obligations on **breach notification**

A Balancing Exercise



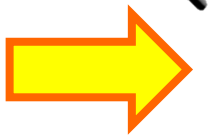
PCPD's Roles – Enforcer + Educator + Facilitator

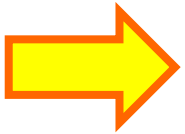
PCPD's Strategic Focus

Fair Enforcement

Engaging

Incentivising





Privacy-friendly Culture

TAKEAWAYS

Proliferation in Fintech causes privacy concerns, e.g. excessive collection, no transparency, unauthorised use, lack of security, bias

Mishandling of personal data harms businesses by customer defection, financial loss, regulatory enforcement, and operation disruption

Accountability and ethics are crucial for striking a balance between data protection and facilitation of businesses and innovation, and for building trust

Download our publications

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

Cloud Computing

This information leaflet aims to advise organisations on the factors they should take into account in considering engaging cloud computing. It explains the relevance of the Personal Data (Privacy) Ordinance (the "Ordinance") to cloud computing. It highlights the importance for a data user to fully assess the benefits and risks of engaging cloud computing and understand the implications for safeguarding personal data privacy.

What is Cloud Computing?

There is no universally accepted definition of cloud computing. For the purpose of this leaflet, it is referred to as a pool of on-demand, shared and configurable computing resources that can be rapidly provided to customers with minimal management efforts or service provider interaction. The cost model is usually based on usage and rental, without any capital investment.

Cloud Computing Engagement and the Ordinance

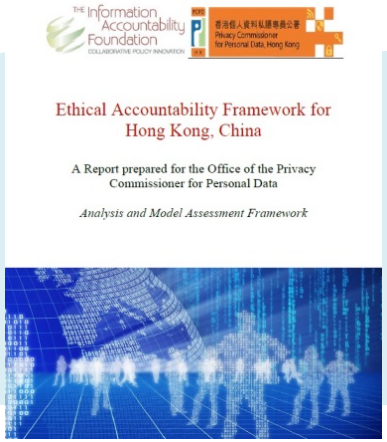
A data user shall comply with the requirements under the Ordinance including the **data protection principles** ("**DPPs**") in Schedule 1. In particular, **DPP2(3)**, **DPP3**, **DPP4** and **Section 65(2)** of the Ordinance are of particular relevance when engaging cloud providers.

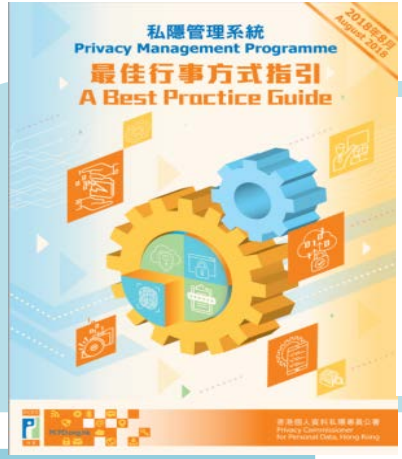
DPP2(3) provides that when a data user engages a data processor, whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data'.

DPP3 provides that personal data should not be used for a new purpose unless prescribed consent (i.e. express and voluntary consent) is obtained from the data subject or his/her "relevant person" as defined under the Ordinance.

DPP4(1) requires a data user to take all reasonably practicable steps to ensure that personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use, having regard to:

Download our publications





PCPD.org.hk

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

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