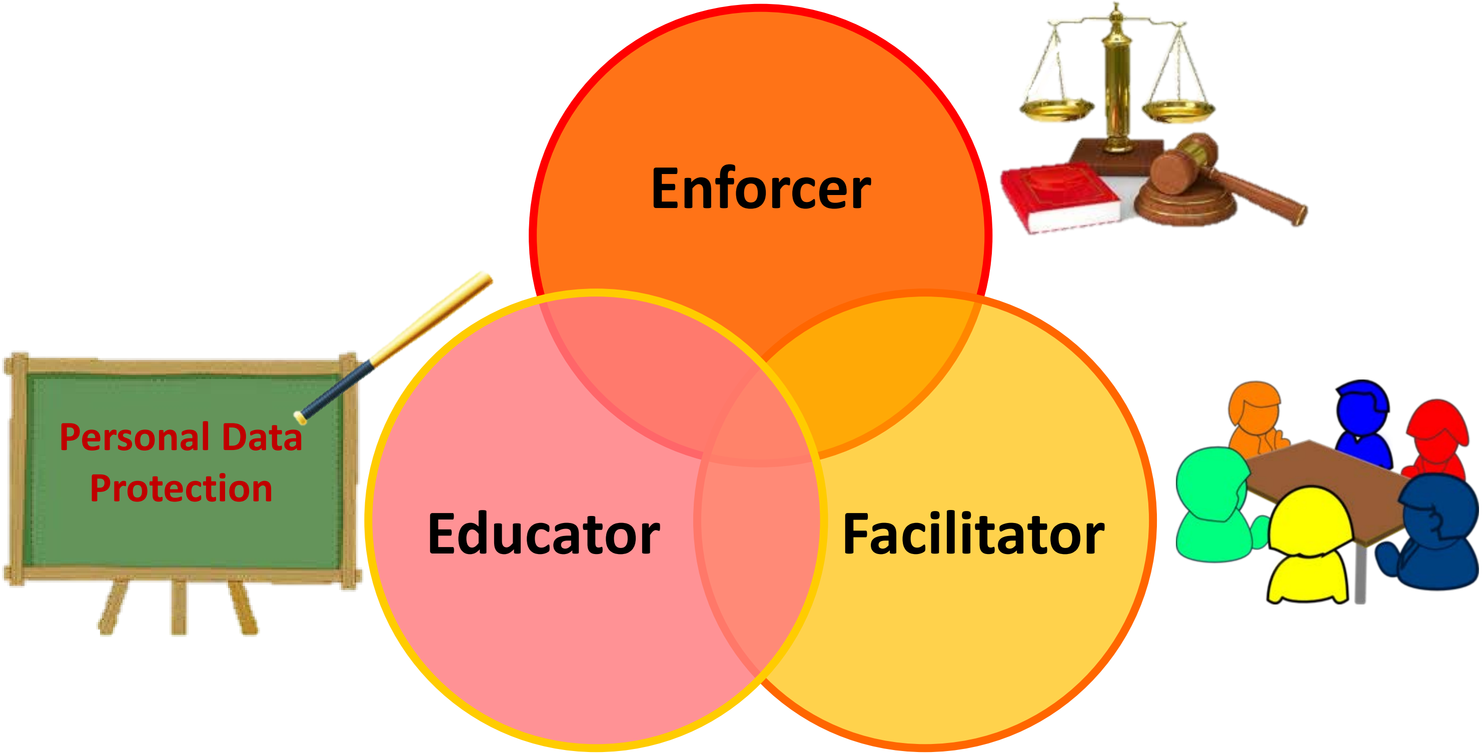
5 June 2019

GDPR and Blockchain : Are they compatible?

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

Role of PCPD



Enforcer

Educator

Facilitator

GDPR and Blockchain: Are they compatible?

- A timely topic with great significance for data protection
- Wide-ranging implications
- Approach the topic from general compliance perspective
- Instead of a verdict, more prudent to discuss how they might/might not be compatible; what can be done

4 characteristics of Blockchains

Transparency

Sharing/ Decentralization

Irreversibility

Disintermediation

Seem to go against many data protection principles

GDPR might also worry the Blockchain community

GDPR: 3 Important Principles

1. Right to Access

- Give people the right to access their data; know how its being handled

2. Right to Rectification

- Allow people to correct data in case of inaccuracy

3. Right to Erasure

- "The right to be forgotten"

3 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

1. Role of Data Controller

= “Data User” under the terminology of the PDPO in Hong Kong

GDPR assigns a lot of responsibility on it to play an active role in data protection (usually organizations or government agencies)

Blockchains decentralized, distributed ledger beyond the control of any single entity/authority
---Who even is the data controller? If such a role even exists?

2. Irreversibility

Once data are recorded, cannot be altered/removed
---stays there for good
---cannot be removed nor amended

GDPR: Right to be forgotten & right of rectification

Potential solution: encryption? Data no longer accessible if encryption key is destroyed

3. Data Retention Period

GDPR: Data cannot be stored for an indefinite period of time
---Exactly what Blockchains do

What can be done if data no longer required or found to be unnecessarily collected?

Data minimization principle: data to be collected have to be relevant and "strictly necessary" for the underlying purposes → restrict innovation?

4. Extra-territorial Effect

GDPR: organizations or companies, even in HK, would need to comply with GDPR under certain conditions (e.g. having an establishment in the EU or targeting services at EU residents)

Blockchain: How do we know when/if a Blockchain will reach any EU citizens, even if initially limited to non-EU parties?

The potential list of incompatibility goes on… However:

- Some common ideas between Blockchains and GDPR
- In a rough sense, both try to achieve similar goals --- with very different methods
- Blockchain: innovative way of data transparency, security, etc, when used properly
- GDPR/Regulators try to do the same

Data Security

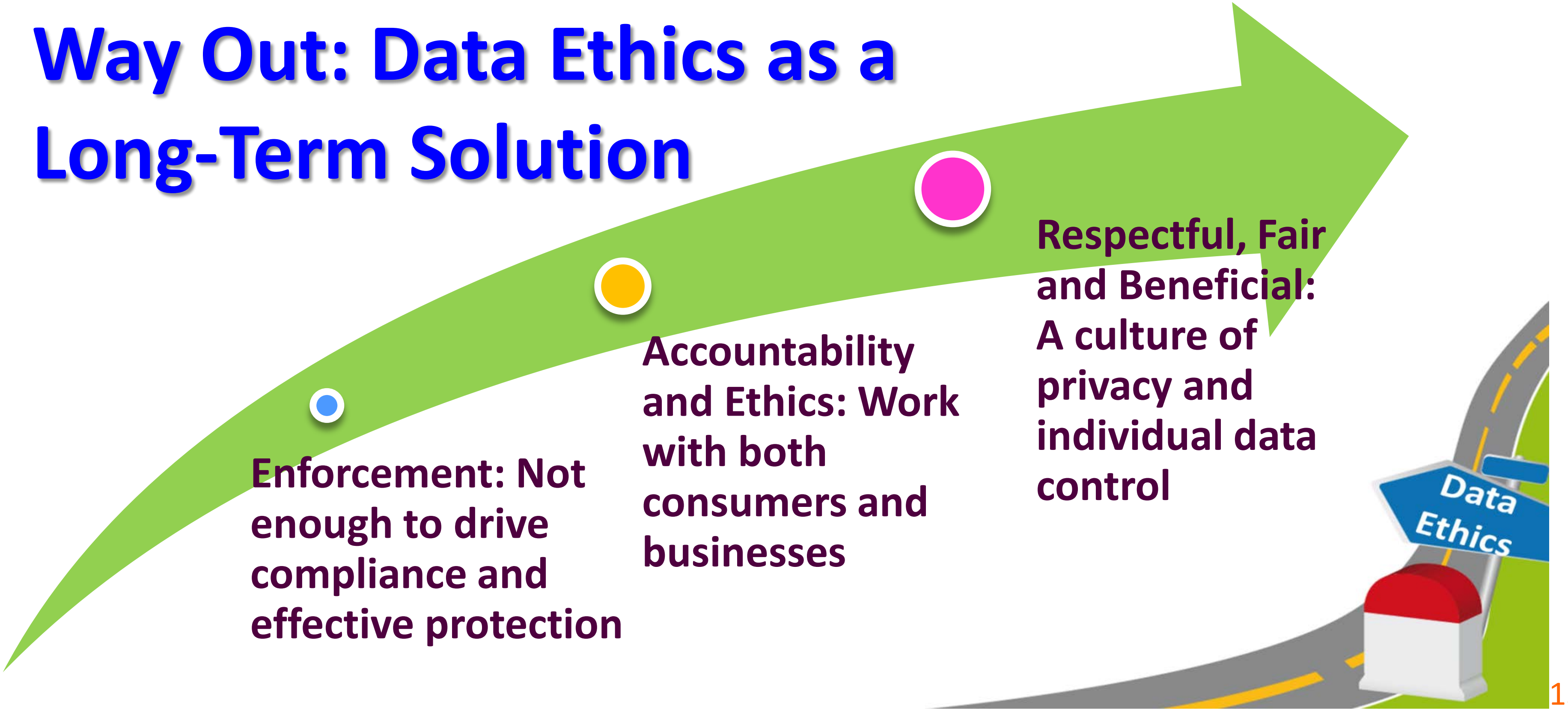
Blockchains: Distributed ledgers remove vulnerabilities in centralized data systems

---Can also store information across systems for improved security

---Remove single point of failure for people to breach and exploit

Similarly, network of data less vulnerable to unauthorized modification

Way Out: Data Ethics as a Long-Term Solution



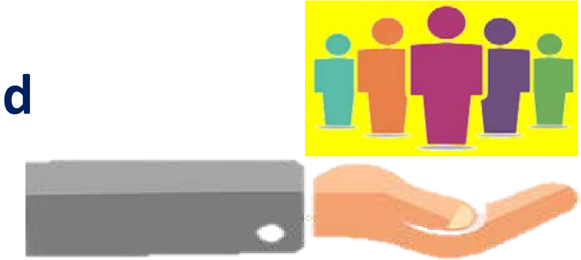
Enforcement: Not enough to drive compliance and effective protection

Accountability and Ethics: Work with both consumers and businesses

Respectful, Fair and Beneficial: A culture of privacy and individual data control

For Business and Organizations Amassing Data

Cannot simply meet the minimum regulatory requirements
---Gap between stakeholders' expectation and data practices

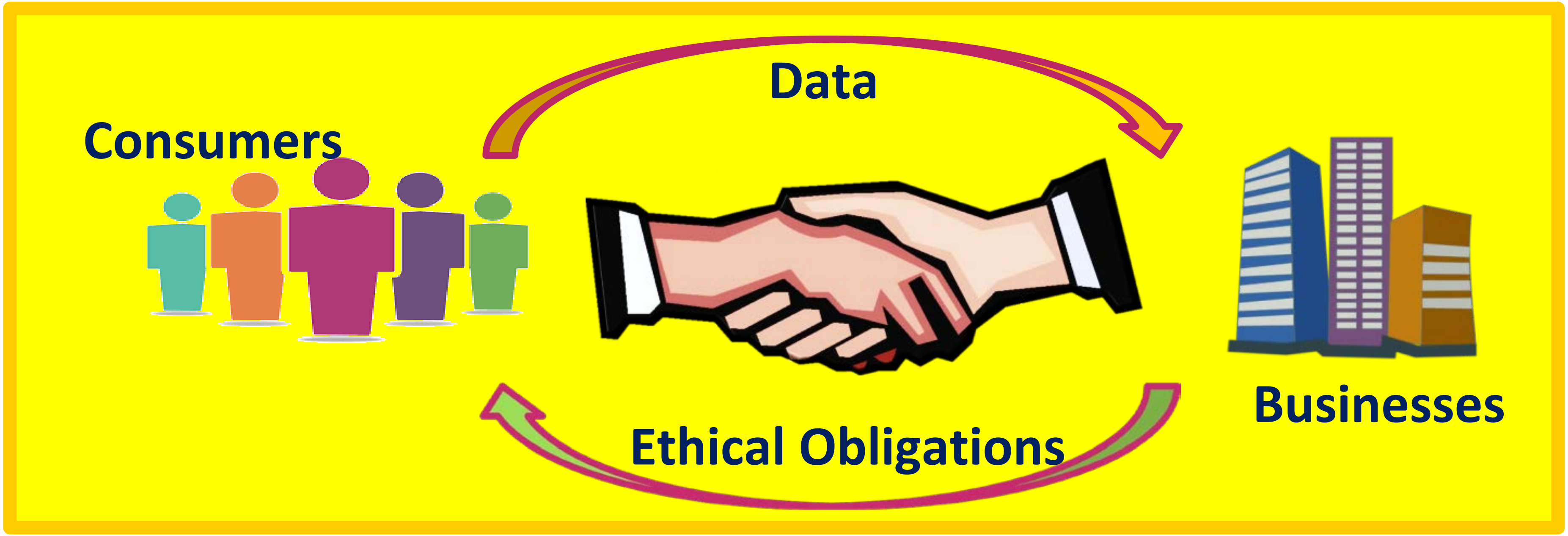


Higher ethical standard meeting stakeholders' expectations as well as laws/regulations
---Data ethnics to bridge the gap

Ethics as a Bridge between Law and Expectation

- Fairness, Respect, Mutual Benefits
- In practice: Genuine Choices, Meaningful Consent, Fair Exchange between Organisations and Individuals
- Data ethics indispensable for building trust; Trust is the bedrock of data economy

Data Ethics & Trust



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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

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
- Recognizes participants in blockchain as "data controllers"

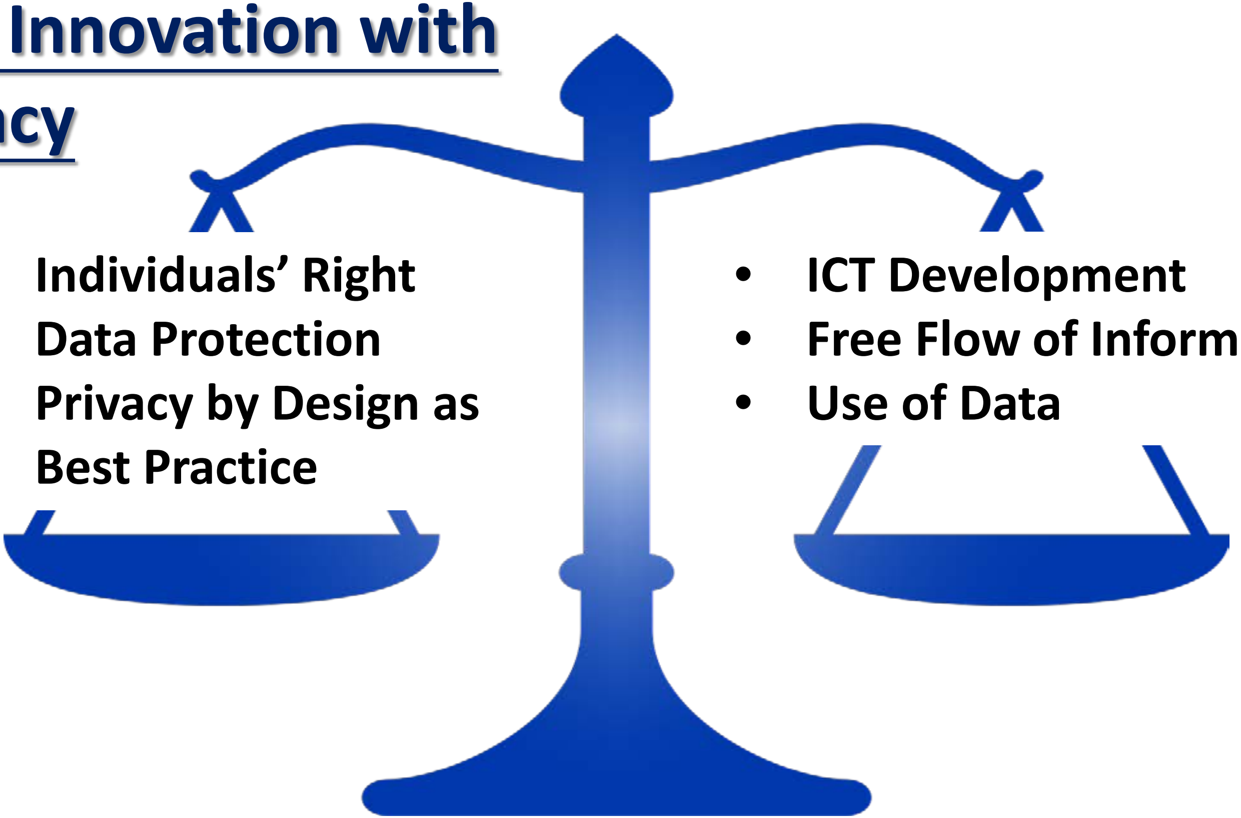
Laws and Enforcements always find it hard to catch-up to latest development

Legislation might be outdated by the time it becomes enforceable after legislation cycle

Goal of PCPD: Work closely with community to ensure respectful, fair, beneficial regulations

Fair Enforcement

Balancing Innovation with Data Privacy

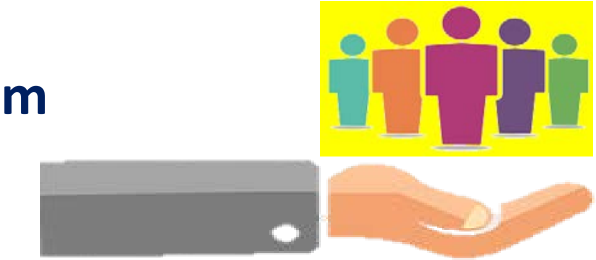


- Individuals’ Right
- Data Protection
- Privacy by Design as Best Practice

- ICT Development
- Free Flow of Information
- Use of Data

Focus on Building Trust

If users do not see enough protection, they might refrain from using the innovation
---Does not bode well for long-term development of information technology



Most ideal scenario of data protection: Not legal documents, not GDPR, not PDPO
---But found on trust and confidence between data users and subjects

> “Trust is the new gold.”

Andrea Jelinek
Chair of European Data Protection Board

Thank you

"Ethical Accountability Framework for Hong Kong, China"

REPORT OF LEGITIMACY OF DATA PROCESSING PROJECT

2018年8月 August 2018

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

香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong
保障、尊重個人資料
Protect,Respect Personal Data
PCPD.org.hk
About PCPD | Data Privacy Law | News & Events | Compliance & Enforcement | Complaints | Legal Assistance | Education & Training | Resources Centre | Enquiry
A Quick Guide
Hot Search
Advanced Search
Keyword Search
RSS
A A A
私隱管理系統
Privacy Management Programme
最佳行事方式指引
A Best Practice Guide
2018年8月
August 2018

Privacy Management Programme: A Best Practice Guide

Privacy Commissioner issued the revised Best Practice Guide on Privacy Management Programme to assist organisations in constructing

What's New More

Reduce Cyberbullying by Nurturing Culture of "Protect, Respect Personal Data" Privacy Commissioner Delivers Panel Presentation at HKU Faculty of Law Symposium on Tackling Cyberbullying

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 Analytica 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

Privacy Commissioner Expresses Concerns Over Typeform's Data Breach Incident (Chinese Version Only)

For Individuals

Think Privacy! Be Smart Online

For Organisations

EU General Data Protection

❑ 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

Copyright