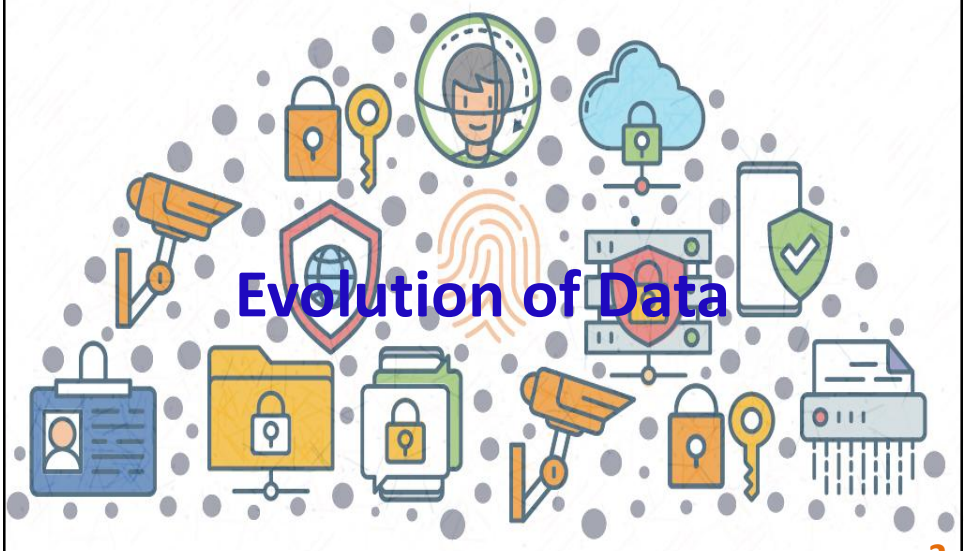
Seminar on Cyber Security and Personal Data Privacy Protection in eHRSS
24 January 2019 | Prince of Wales Hospital

Data Breaches and Cybersecurity

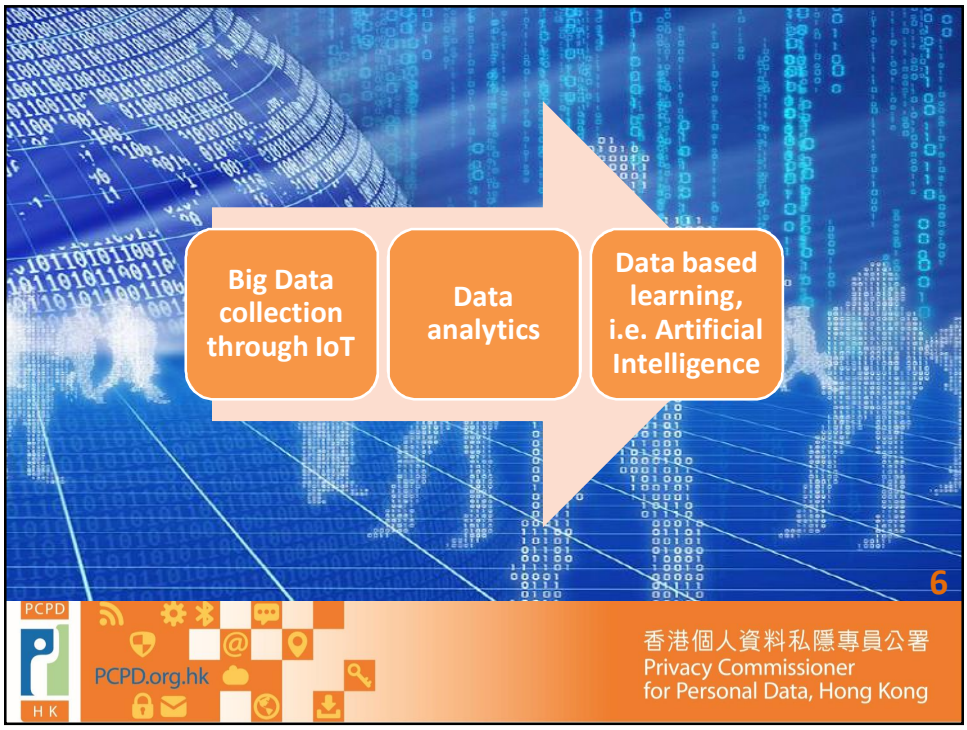


Evolution of Data


A3
星島日報
一九九八年十一月五日
星期四
售樓處設在「銅鑼灣世貿中心25字樓」
並於明日上午10時正開售，敬請留意！
明日公開發售共188個單位
港匯豪園
WATERFRONT SOUTH
由電腦抽籤排列揀樓次序之
申請表號碼
揀樓次序
身份證號碼／商業登記證號碼
SA0808 00764 D670151(6)
SA0809 00701 D394775(J)
SA0810 00475 D433676(4)
SA0811 00559 K185965(A)
SA0812 00153 D525178(9)
SA0813 00071 G205170(8)
SA0814 00891 G080280(7)
PCPD
HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong
3


Internet of Things
PCPD
HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong
4


Big Data
Contact addresses and details
Identifiers
Contacts and accounts
Relationships
Support history
Call centre logs
Unstructured documents
Email text and sentiment
Social media sentiment
Order history
5
PCPD
HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner for Personal Data, Hong Kong


Big Data collection through IoT
Data analytics
Data based learning, i.e. Artificial Intelligence
6
PCPD
HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner for Personal Data, Hong Kong

"Information is the oil of the 21st century, and analytics is the combustion engine."

(Peter SONDERGAARD – Gartner)

Source: DataWorks Summit/ Hadoop Summit

How much is your data worth?

Category	Price
Music Streaming Account	$2.75
Movie Streaming Account	$2.75
TV Shows Steaming Account	$1.00 - 3.00
Payment Credentials	$1.50
Social Security Number	$1.00
Driver's License	$20.00
Credit Card	$8.00 - $22.00
Email Address & Password	$0.70 - $2.30
Medical Record from Large Scale Attack	$1.50 - $10.00
Complete Medical Record	Up to $1,000.00

Source: https://keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html

PCPD HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Figures of Data Breach in 2018

2,694,400,000
records exposed or stolen globally in 2018

- Every Day - 7.85M
- Every Hour – 327K
- Every Minute - 5.46K
- Every Second - 91

Sources: Bloom & Identity Theft Resources Centre

Recent Data Breach Incidents

Companies involved	Number of affected subjects
Marriott International	383,000,000
Twitter	330,000,000
My Fitness Pal	150,000,000
Facebook	147,000,000
Quora	100,000,000
Firebase	100,000,000
My Heritage	92,000,000
Uber	57,000,000
Ticket Fly	27,000,000
Google+	500,000
British Airways	380,000

PCPD HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

PCPD.org.hk

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

Personal Data (Privacy) Ordinance

PCPD.org.hk

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

What is "Personal Data"?

(a) relating directly or indirectly to a living individual

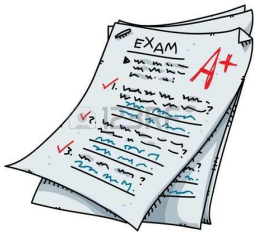
(b) practicable for the identity of the individual to be directly or indirectly ascertained

(c) in a form in which access to or processing is practicable

Personal Data?

Gossip

Fingerprint



Exam questions and answers

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

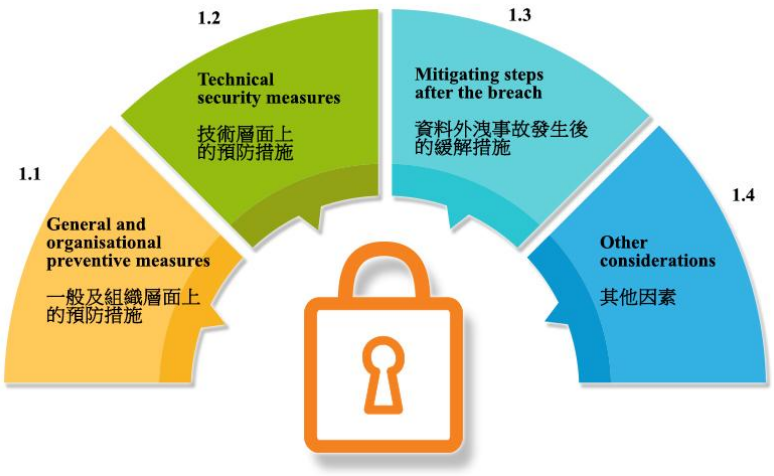
6 Data Protection Principles

4. Data Security Principle

Data user shall take all practicable steps to ensure that personal data held by them are protected against unauthorised or accidental access, processing, erasure, loss or use.

PCPD HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

What is "all practicable steps"?



What is "all practicable steps"?

Personal data privacy protection as part of the corporate governance responsibilities, covering business practices, operational processes, policies and training

Comprehensive and on-going review and monitoring process; build a robust privacy infrastructure

1. General and Organisational Preventive Measures

Open and transparent information privacy policies and practices

Top management commitment, a top-down business imperative throughout the organisation

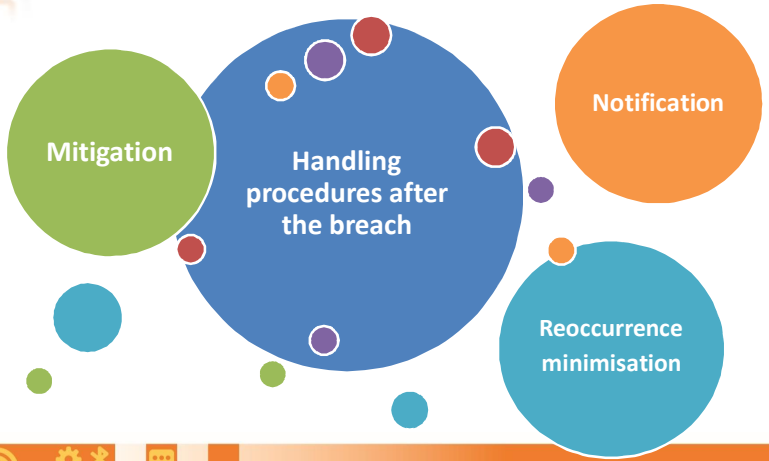
What is “all practicable steps”?

2. Technical Security Measures

- Hardware security, e.g. information system, network infrastructure, etc
- Policies and procedures for regular review of security systems
- Security measures and steps for system login, data transmission and storage, and adoption of international standards and technology, e.g. hashing, encryption, etc

What is “all practicable steps”?

3. Mitigating Steps after the Breach



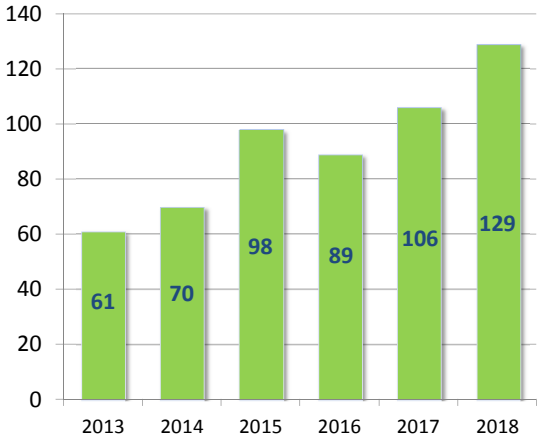
What is “all practicable steps”?

4. Other Considerations

- Nature, size and resources of the data user
- Likelihood of adverse consequences for affected individuals
- Complexity of its operations of the data user and its business model
- Amount and sensitivity of personal data held

PCPD HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Data Breach Notifications Received



Year	No. of Data Subjects Involved
2013	90,000
2014	47,000
2015	871,000
2016	104,000
2017	3,866,000
2018	2,387,000

Common Types of Data Breach Incidents

1. loss of physical documents or portable device
2. IT systems with improper settings or being attacked by hackers or malwares
3. missent of emails or letters
4. employees' non-compliance with data security policy
5. improper disposal of personal data

PCPD HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Cases in Medical Sector

CASE 1

- scrap paper was used for printing appointment slips and distributed to a patients
- other patients' personal data were shown on the back of the appointment slips

CASE 2

- an external component (with patients' personal data saved in it) of an apparatus in a hospital was stolen
- the device was not locked by a chain lock
- no change of the log-in password default upon manufacture

Cases in Medical Sector

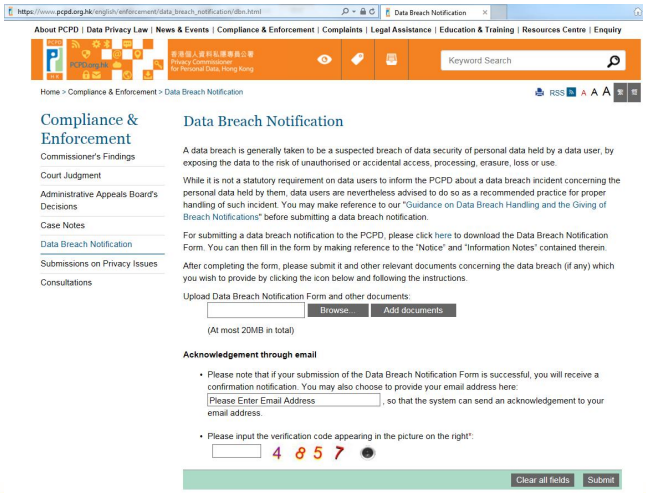
CASE 3

- hospital waste containing patients' personal data were found abandoned on the street outside a shredding factory which was a service provider of the hospital

Data Security in eHRSS

- Ensure that when authorised staff log into the eHRSS, eHR shown on the computer screen will not be seen by unrelated third parties.
- Keep the eHR downloaded or printed from the eHRSS safely.
- Guidelines on the use of portable storage devices should be formulated to avoid leakage of personal data.
- Adopt appropriate measures to ensure that healthcare providers' data systems are adequately safeguarded and properly functioned.

How to report a data breach to PCPD



4 Steps for Data Breach Handling and Notifications

Collecting Information Immediately

Immediate gathering of essential information relating to the breach including:

- When and where did the breach take place?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind and extent of personal data was involved?
- How many data subjects were affected?

29

4 Steps for Data Breach Handling and Notifications

Contacting the Interested Parties & Adopting Containment Measures

Interested parties may include:

- The law enforcement agencies
- The relevant regulators (e.g. Privacy Commissioner for Personal Data, Hong Kong (the "Commissioner"))
- The Internet companies
- IT experts

30

4 Steps for Data Breach Handling and Notifications

Assessing the Harm

Assessing the potential harm caused by a data breach, for examples:

- Threat to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationship
- Loss of business and employment opportunities

4 Steps for Data Breach Handling and Notifications

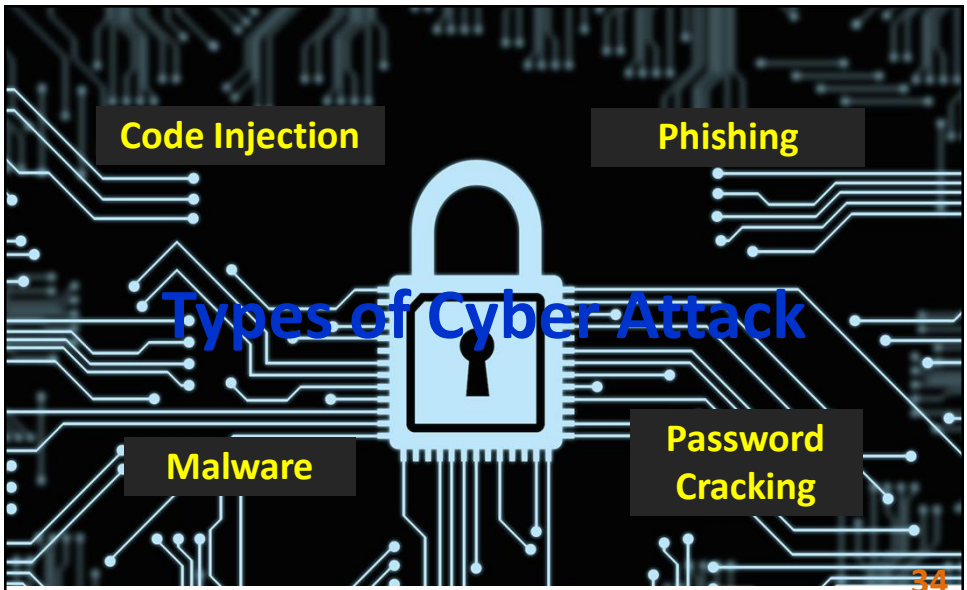
Considering the Giving of Notification

When real risk of harm is reasonably foreseeable in a data breach, the data user should consider:

- Notifying the affected data subjects and the relevant parties
- The consequences for failing to give notification

Actions to be taken by PCPD

- PCPD would assess the information provided in the Data Breach Notification and consider whether a compliance check or compliance investigation is warranted



Incident 1: Customer databases and servers of a toy maker were hacked

BACKGROUND

- leaked personal data of about 5 million parents and 6.6 million related children
- data included parents' names, email addresses, children's names, gender, and full dates of birth; and chat and voice messages and photos

Incident 1: Customer databases and servers of a toy maker were hacked

CAUSES

- no basic security measures: countermeasures to prevent SQL injections, installing web application firewalls, and encrypting personal data
- IT security policies and guidelines did not retroact upon old systems
- failed to monitor the implementation of its IT security policies and guidelines and update time timely

PCPD HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 1: Customer databases and servers of a toy maker were hacked

REMEDIAL ACTIONS

- stopped collecting the children's dates and months of birth during account registration
- enhanced its protective measures against unauthorised data access
- promulgated a new Data Security Policy
- formed a Data Security Governance Board

Incident 2: Network-attached storage servers of a university were hacked

BACKGROUND

- files containing personal data of 15,547 patients and 200 students and/or staff were maliciously encrypted by a hacker
- the university was blackmailed for bitcoins in exchange for the decryption key

CAUSES

- lack of proper security patches on the servers → allowed the hacker to use ransomware to exploit the security vulnerabilities of some servers running older versions of the operating system

Incident 2: Network-attached storage servers of a university were hacked

REMEDIAL ACTIONS

- setting up a new server following the university's guidelines on server protection
- performing regular maintenance on the new server
- identifying unprotected file servers used by the faculty, and protecting them behind its firewall
- conducting a departmental information security review
- reinforcing awareness of its departmental IT staff members of data security

Incident 3: Customer databases of travel agencies were hacked

BACKGROUND

- databases of several travel agencies containing personal data of about 200,000 customers were encrypted by a hacker who demanded a ransom in exchange for decryption key

REMEDIAL ACTIONS

- enabling web application firewall
- adopting two-factor authentication for remote access
- encrypting the customer database
- creating an offline backup, conducting penetration testing and vulnerability scanning regularly, etc.

Risks of Engaging Data Processors

Service providers *(as data processors)* may keep data longer than necessary *[DPP 2(3)]*

Request for data deletion ≠ Immediate deletion

Risks of Engaging Data Processors

Unauthorised access to customer and business data (e.g. hacking, data breach) *[DPP 4(2)]*

Risks of Engaging Data Processors

"Secondary uses" of data with or without data users' knowledge
[DPP 3 & s.65(2)]

Incident 4: Customers' personal data of a bank was downloaded without authorisation

BACKGROUND

- a contractor downloaded 964 data files (with 210,000 customers' personal data) from the bank's computer workstation to his mobile device without authorisation
- measures implemented at the material time:
  - ✓ contractual control, confidentiality agreement
  - ✓ requiring the contractor to work in the bank office
  - ✓ data loss prevention system controls
  - ✓ monitoring tools to detect abnormal activities

PCPD HK
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Incident 4: Customers' personal data of a bank was downloaded without authorisation

CAUSES

- misconfiguration of its data loss prevention system → failed to block the transfer of data from computer workstations to portable devices

REMEDIAL ACTIONS

- re-configuring data loss prevention system controls
- enhancing inadvertent data disclosure and end-point security tools
- monitoring external data transfers
- only dummy or masked personal data to be used for testing and system development

Lesson Learnt to Prevent Recurrence

- improvement of security
- control of access rights
- revision or promulgation of privacy policy and practice
- effective detection of data breach
- strengthening of monitoring and supervision
- provision of on-the-job training

LESSON LEARNT

Privacy Issues in the Age of Big Data, Artificial Intelligence & Internet of Things

- convert data collection
- tracking and monitoring
- re-identification
- profiling, unfairness and discrimination
- low transparency
- unpredictability
- cybersecurity

Privacy-based Solutions

Promoting Data Ethics

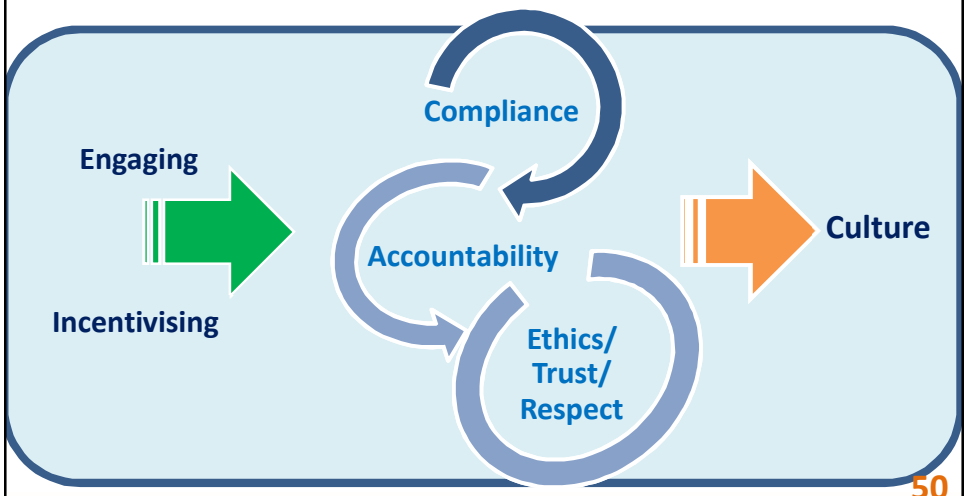
Privacy Management Programme –

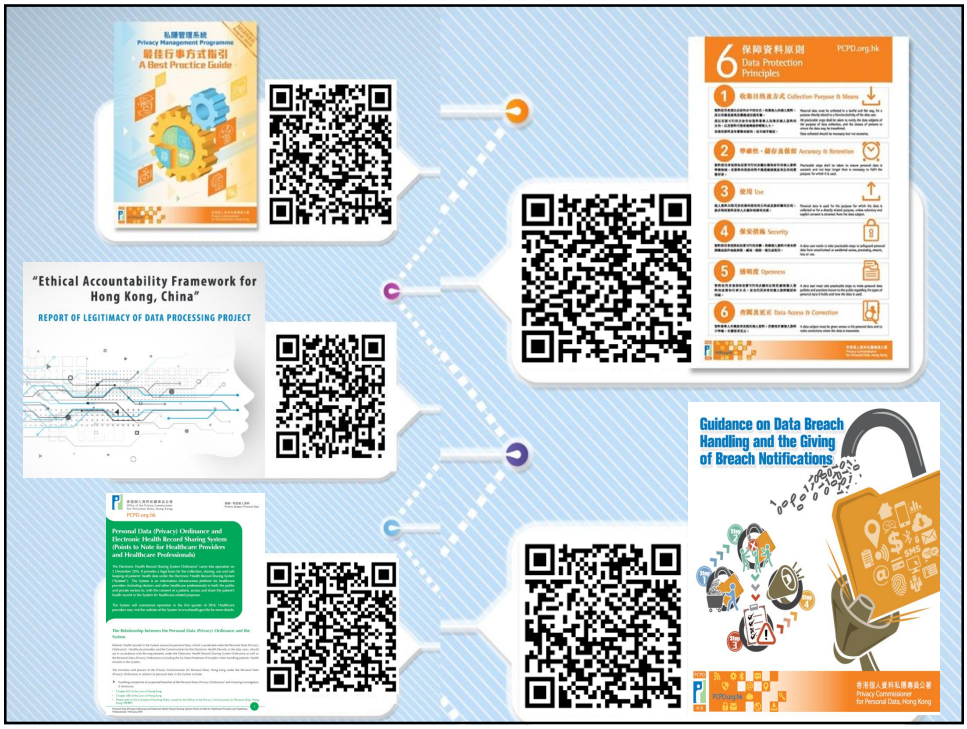
paradigm shift from compliance to ***accountability***

Data ethics –

ethical & fair processing of data – due consideration of the rights, interests and freedoms of individuals

PCPD's Strategic Focus





Contact Us

- ❑ Website **www.pcpd.org.hk**
- ❑ Email **enquiry@pcpd.org.hk**
- ❑ Tel **2827 2827**
- ❑ Fax **2877 7026**
- ❑ Address **Room 1303, 13/F, Sunlight Tower 248 Queen's Road East Wanchai, Hong Kong**

PCPD H K PCPD.org.hk 香港個人資料私隱專員公署 Privacy Commissioner for Personal Data, Hong Kong