Webinar on Cyber Security and Personal Data Privacy Protection in eHRSS

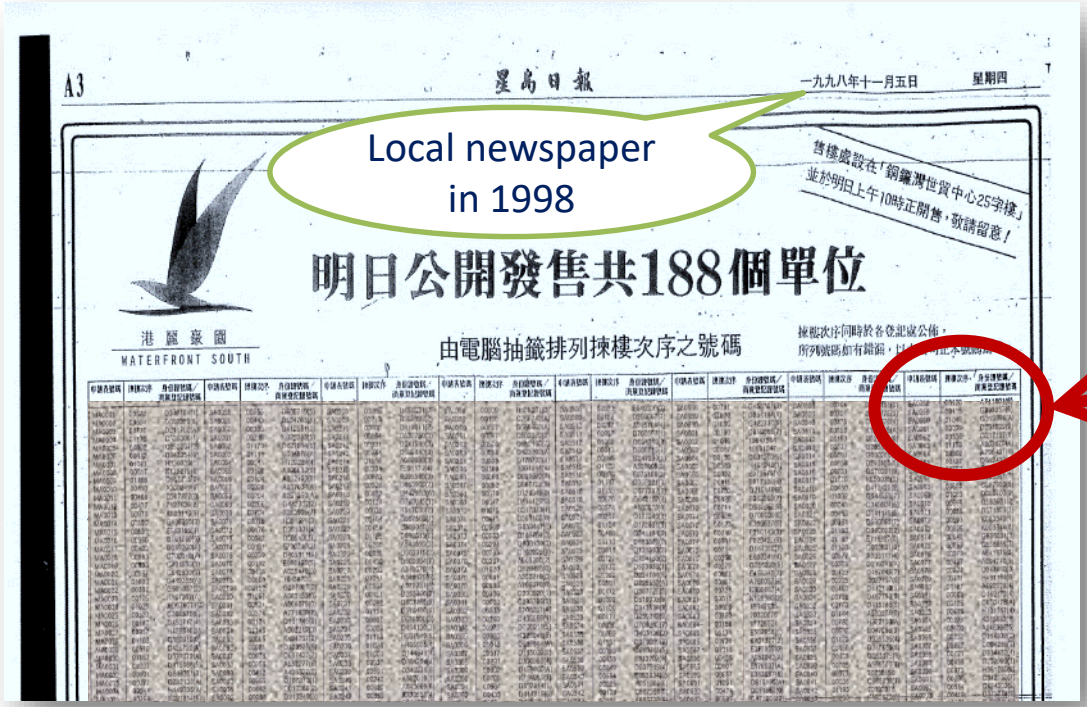
13 August 2020

Joanna CHAN
Senior Personal Data Officer

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

Data covers everyone of us from cradle to grave

Our sensitive personal data might even be publicly disclosed



Local newspaper in 1998

[Property Lottery Result Announcement in 1998]

申請表號碼	揀樓次序	身份證號碼／商業登記證號碼
SA0808	00764	D[redacted]6)
SA0809	00701	D[redacted])
SA0810	00475	D[redacted])
SA0811	00559	K[redacted]A)
SA0812	00153	D[redacted]0)
SA0813	00871	C[redacted]3)
SA0814	00891	C[redacted]7)

Full HKID Card number

Source: Asia Pacific Privacy Authorities

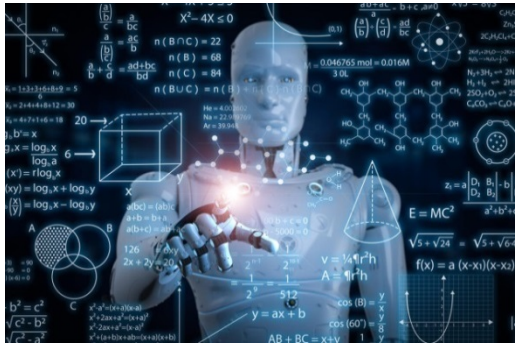
Healthcare Trend

- Informed and demanding patients are now partners in their own healthcare
- Digitized medicine
- Telemedicine
- Wearables and Apps
- Big Data
- Impact of behaviors on corporate reputation → trust

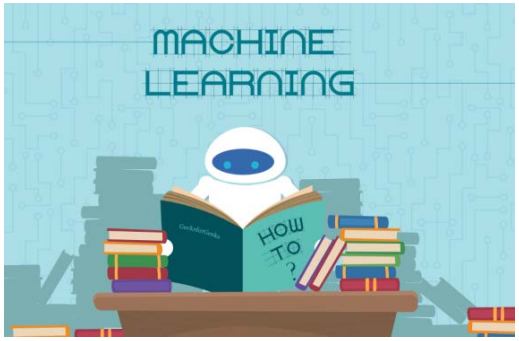
Source: SCMP

Source: https://www2.deloitte.com/cn/en/pages/life-sciences-and-healthcare/articles/healthcare-and-life-sciences-predictions-2020.html

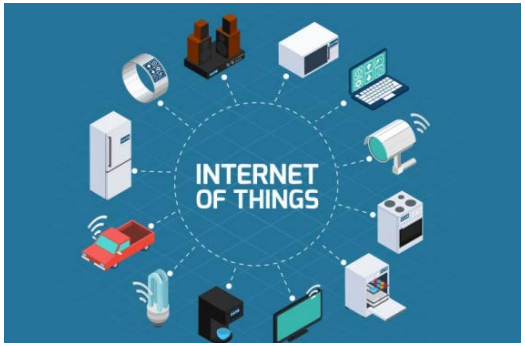
Advancement in Technology



Robotics



Machine learning



Internet of Things

Artificial Intelligence

Autonomous vehicles

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

Even beggars may collect your personal data through e-wallets

Source: 中國評論通訊社 (CRNTT.com), 2017

Behind the huge value of e-commerce is huge volume of personal data

Sales on 'Double 11 Day' on an e-commerce platform in mainland

2017: RMB 168.2 billion sales

2018:
29% increase year-on-year

2019:
26% increase year-on-year

Volume of data is growing exponentially

"There were 5 Exabytes of information created between the dawn of civilization through 2003, but that much information is now created every 2 days."

Eric Schmidt, Google, 2010
(Source: World Economic Forum)

(Note: 1 Exabyte = 1 billion Gigabytes)

The proliferation of devices such as PCs and smartphones worldwide, increased Internet access … has contributed to the doubling of the digital universe within the past two years alone.

IDC, 2012
(Source: DELL Technologies - IDC Digital Universe study)

IDC predicted that the "*Global Datasphere*" would grow from 33 Zettabytes in 2018 to 175 Zettabytes by 2025.

IDC, 2018
(Source: IDC White Paper "The Digitization of the World From Edge to Core")

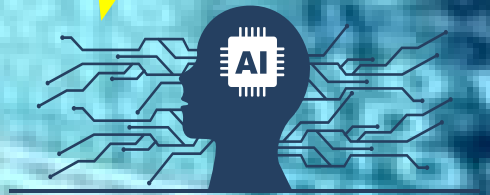
(Note: 1 Zettabyte = 1,000 Exabytes = 1 trillion Gigabytes)

Data is the Lifeblood of a 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



Positive Impacts of AI & Big Data

Enormous Economic Value

- Improve efficiency
- Simplify process
- Facilitate innovation
- Increase accuracy

Value of data is increasing

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

Peter Sondergaard, Gartner Research, 2011
(Source: Medium.com)

"The world's most valuable resource is no longer oil, but data."

The Economist, 2017
(Source: Economist.com)

"Data is the most valuable asset of Alibaba.
The key objective of Tao Bao is not selling goods, but collecting retail and manufacturing data.
The key objective of Ant Financial is establishing a credit scoring system.
Our logistics operation is not aimed at delivering goods, but aggregating data."

Jack Ma, Alibaba, 2014
(Source: 人民網 (People.com.cn) [Originally in Chinese])

How much is your data worth?

Category	Price (USD)
Cloned VISA with PIN	$25
Credit Card details, account balance up to $1,000	$12
Credit Card details, account balance up to $5,000	$20
Stolen online banking logins, minimum $100 on account	$35
Stolen online banking logins, minimum $2,000 on account	$65
Stolen PayPal account details, minimum $100 on account	$198.56
Driving license	$70
Bank statement	$25
Hacked Facebook account	$74.5
Hacked Instagram account	$55.45
Hacked Gmail account	$155.73

Source: https://www.privacyaffairs.com/dark-web-price-index-2020/

How about medical data?

- the resale value of a medical record is from $70 to $100 each, depending on how comprehensive it is and what type of patient it belongs to
- the value of certain records depends on the buyers intent, if the 'intent' is to get money by blackmailing the victim, the medical record would need to have extremely sensitive information included
- one of the newer trends is stealing the identities of doctors (selling on the dark web for $500)
- documents on sale include malpractice insurance documents, medical diplomas, board recommendations, medical doctor licences
- using this stolen information they can forge the identities of doctors and submit fraudulent insurance claims or obtain prescriptions for controlled drugs

Source:https://www.totalprocessing.com/totalprocessing.com/public/blog/how-much-is-your-data-worth-on-the-dark-web

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

Evolving Nature of Personal Data

- Privacy / personal data protection laws in most jurisdictions tend to focus on the protection of "personal data" – data that **identifies** an individual, or renders the person **identifiable**

- E.g. Personal Data (Privacy) Ordinance defines "personal data" as- any data:

  *"… from which it is practicable for the **identity** of the individual to be directly or indirectly **ascertained**."*

Personal Data - expanding

"Personal data" now incorporates a **constantly-expanding array of information** under many privacy / personal data protection laws, e.g.-

Location data	• GPS location • Proximity to Wi-Fi or Bluetooth beacons • Proximity to nearby mobile network towers
IP address	• Internet protocol address that identifies a computer • May reveal approximate location of a user
Device identifier	• Unique information identifying a mobile device • e.g. MAC address, IMEI number

Personal Data – expanding

Internet activity	• Browsing histories • Search histories
Biometric information	• Facial, fingerprint, iris and retina images • Gaits • Genetic or DNA information
Consumer data	• Purchase histories • Credit histories
Health & medical information	• Medical conditions • Frequency of visiting doctors • Contact-tracing information in times of COVID-19 pandemic

Relationship between the Personal Data (Privacy) Ordinance and the eHRSS

- Patients' health record in the eHRSS amounts to personal data, which is protected under the Personal Data (Privacy) Ordinance.
- Both Healthcare providers and the Commissioner for Electronic Health Record are data users.

Functions and powers of PCPD in relation to the eHRSS

- handling complaints of suspected breaches of the PDPO and initiating investigation if necessary
- carrying out an inspection of the eHRSS
- providing guidance on personal data privacy in relation to the eHRSS to citizens and healthcare providers
- handling any data breach notification in relation to the eHRSS

6 Data Protection Principles

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.

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

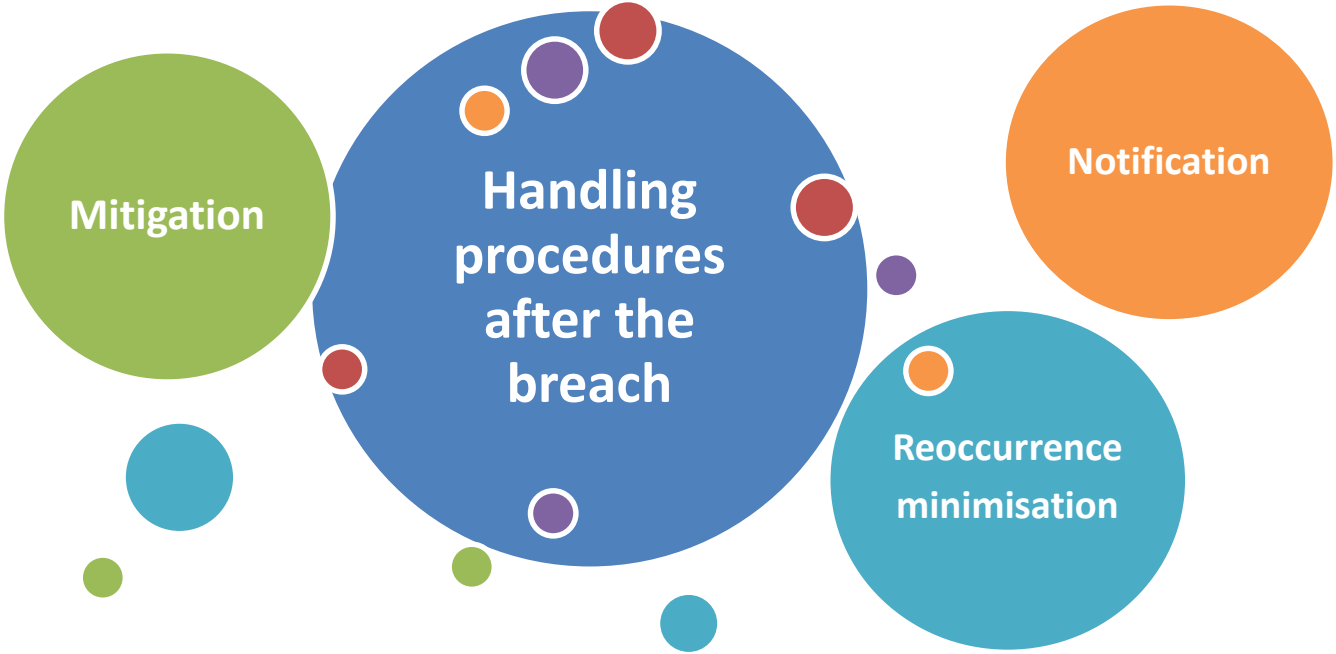
- Hardware security, e.g. information system, network infrastructure, etc
- Policies and procedures for regular review of security systems
- Security measures and steps for system login, data transmission and storage, and adoption of international standards and technology, e.g. hashing, encryption, etc

- World's first international standard for managing privacy information
- Building on ISO 27001 and ISO 27002
- Assisting in compliance with personal data protection laws

- Four core parts:
  - ❖ Personal information management system
  - ❖ Information security techniques and good practices
  - ❖ Guidance for PII controllers (i.e. data users)
  - ❖ Guidance for PII processors (i.e. data processors)

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

Failed to take all practicable steps…

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

Failed to take all practicable steps…

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.

Publications

Target：Participants of the eHRSS

Content covers：

- **The relationship between the Ordinance and the eHRSS**
- **10 privacy protection tips**
- **Complaint Channels**

Download >>

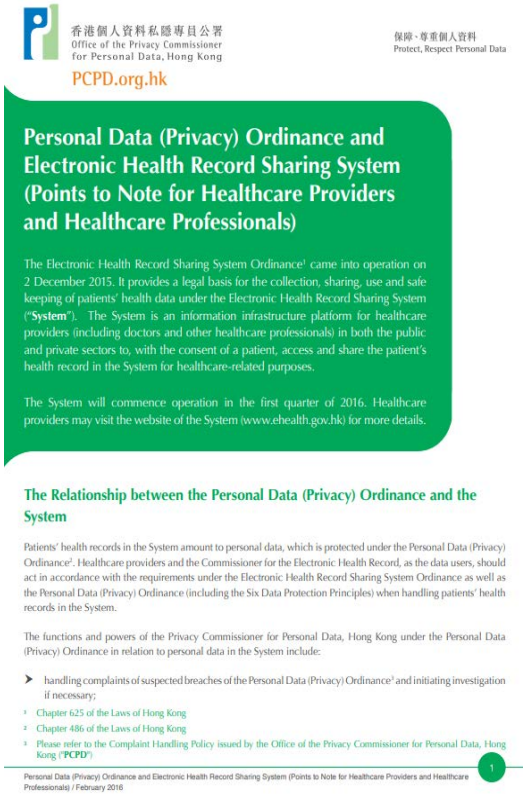
Publications

Target ： Healthcare providers & healthcare professionals

Content covers：

- **The relationship between the Ordinance and the eHRSS**
- **Points to Note for Healthcare Providers and Healthcare Professionals**
- **Complaint Channels**
- **Action list for Healthcare Providers before joining the eHRSS for protection of personal data privacy**

Download >>


香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong
PCPD.org.hk
保障、尊重個人資料
Protect, Respect Personal Data

Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals)

The Electronic Health Record Sharing System Ordinance[1] came into operation on 2 December 2015. It provides a legal basis for the collection, sharing, use and safe keeping of patients' health data under the Electronic Health Record Sharing System ("**System**"). The System is an information infrastructure platform for healthcare providers (including doctors and other healthcare professionals) in both the public and private sectors to, with the consent of a patient, access and share the patient's health record in the System for healthcare-related purposes.

The System will commence operation in the first quarter of 2016. Healthcare providers may visit the website of the System (www.ehealth.gov.hk) for more details.

The Relationship between the Personal Data (Privacy) Ordinance and the System

Patients' health records in the System amount to personal data, which is protected under the Personal Data (Privacy) Ordinance[2]. Healthcare providers and the Commissioner for the Electronic Health Record, as the data users, should act in accordance with the requirements under the Electronic Health Record Sharing System Ordinance as well as the Personal Data (Privacy) Ordinance (including the Six Data Protection Principles) when handling patients' health records in the System.

The functions and powers of the Privacy Commissioner for Personal Data, Hong Kong under the Personal Data (Privacy) Ordinance in relation to personal data in the System include:

- handling complaints of suspected breaches of the Personal Data (Privacy) Ordinance[3] and initiating investigation if necessary;

[1] Chapter 625 of the Laws of Hong Kong
[2] Chapter 486 of the Laws of Hong Kong
[3] Please refer to the Complaint Handling Policy issued by the Office of the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**").

Personal Data (Privacy) Ordinance and Electronic Health Record Sharing System (Points to Note for Healthcare Providers and Healthcare Professionals) / February 2016

Data Breach

What is a data breach?

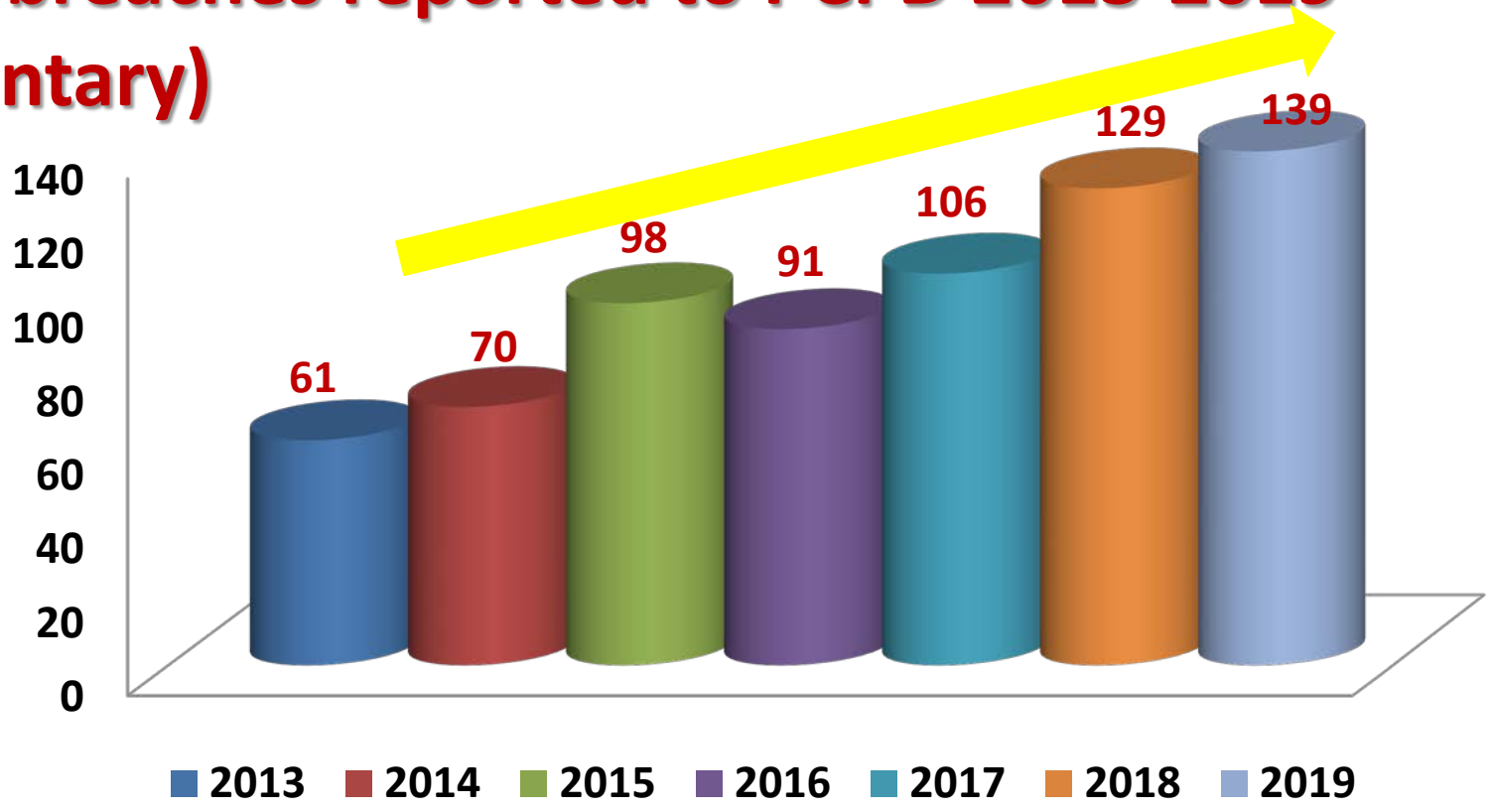
- ***Data Protection Principle 4:*** Data users shall take all practicable steps to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data.

- ***Definition of "personal data breach":*** A data breach is a suspected breach of security exposing personal data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

Common Types of Data Breach Incidents

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

Data breaches reported to PCPD 2013-2019 (voluntary)



How to report a data breach?

- Report to the data subjects affected
- Report to the Commissioner by means of the "Data Breach Notification Form"
- Submit the completed form to us online, by fax, in person or by post
- Details:

  https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

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?

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

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

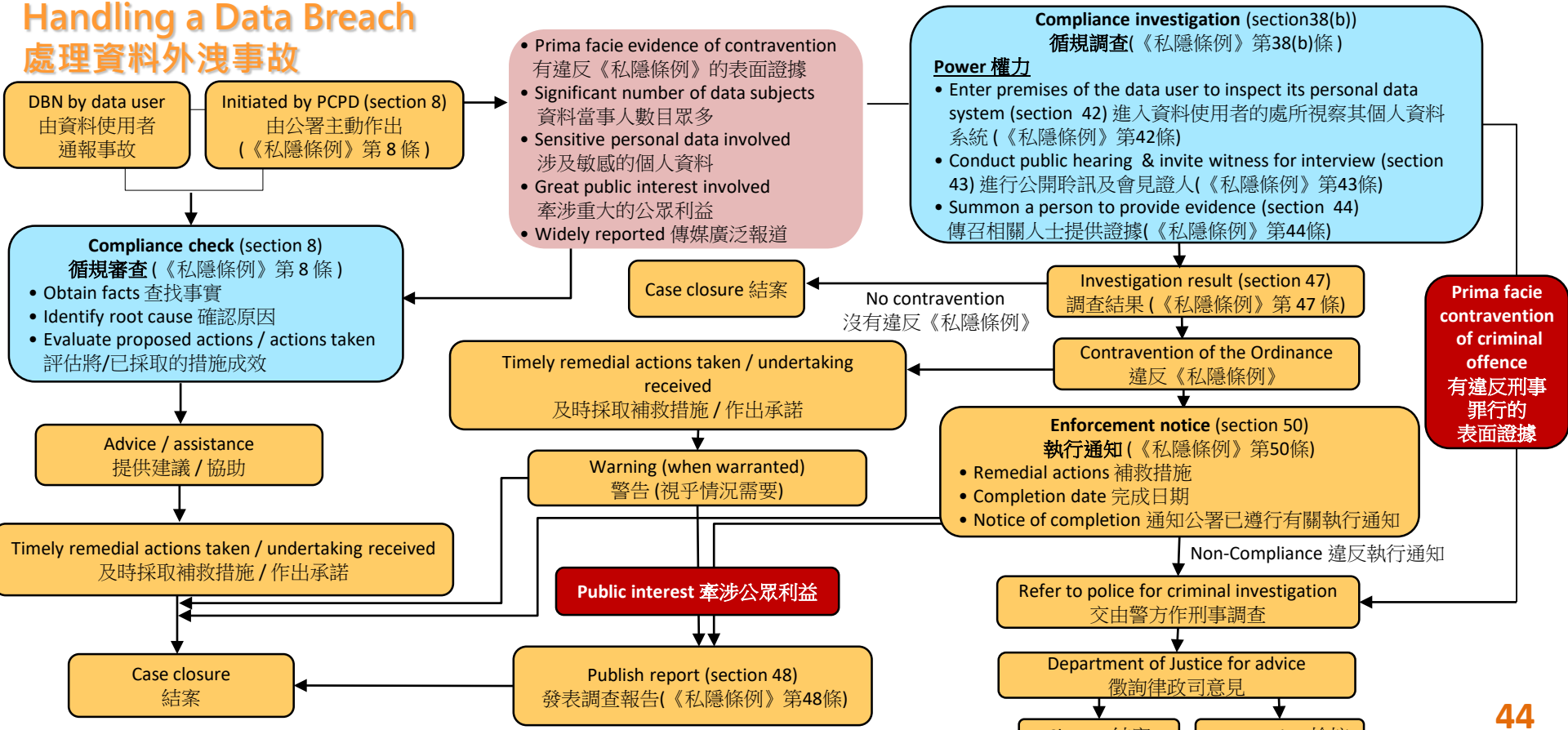
4 Steps for Data Breach Handling and Notifications

Considering the Giving of Notification

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

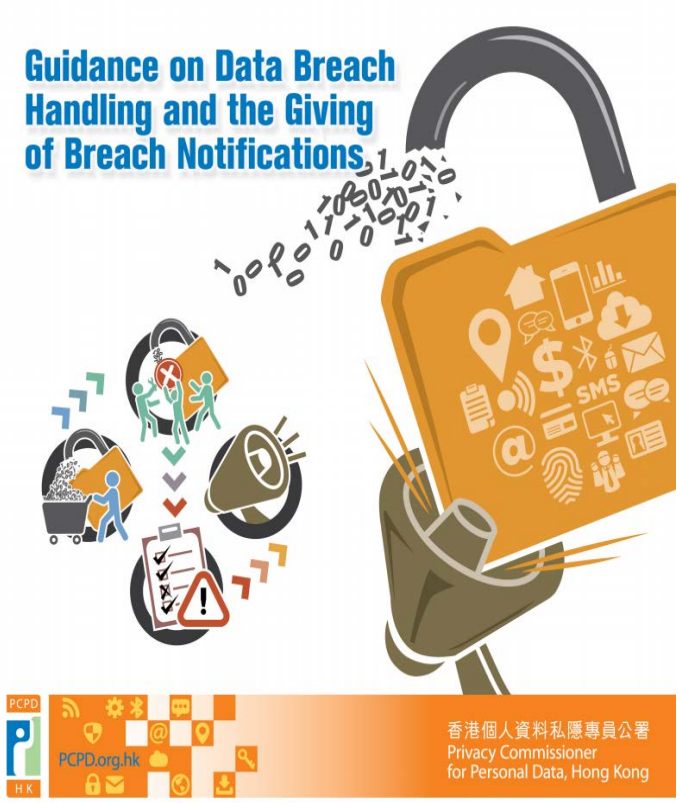
- Notifying the affected data subjects and the relevant parties
- The consequences for failing to give notification

Handling a Data Breach
處理資料外洩事故



Publications

Download >>




Cyber Attack

Case 1: Network-attached storage servers of a university were hacked

BACKGROUND

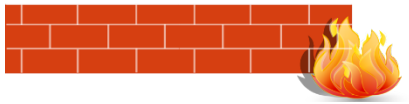
- files containing personal data of 15,547 patients and 200 students and/or staff were maliciously encrypted by a hacker
- the university was blackmailed for bitcoins in exchange for the decryption key

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

Case 1: Network-attached storage servers of a university were hacked

REMEDIAL ACTIONS

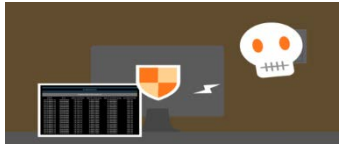


- setting up a new server following the university's guidelines on server protection
- performing regular maintenance on the new server
- identifying unprotected file servers used by the faculty, and protecting them behind its firewall
- conducting a departmental information security review
- reinforcing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

Case 2: Customer databases of travel agencies were hacked

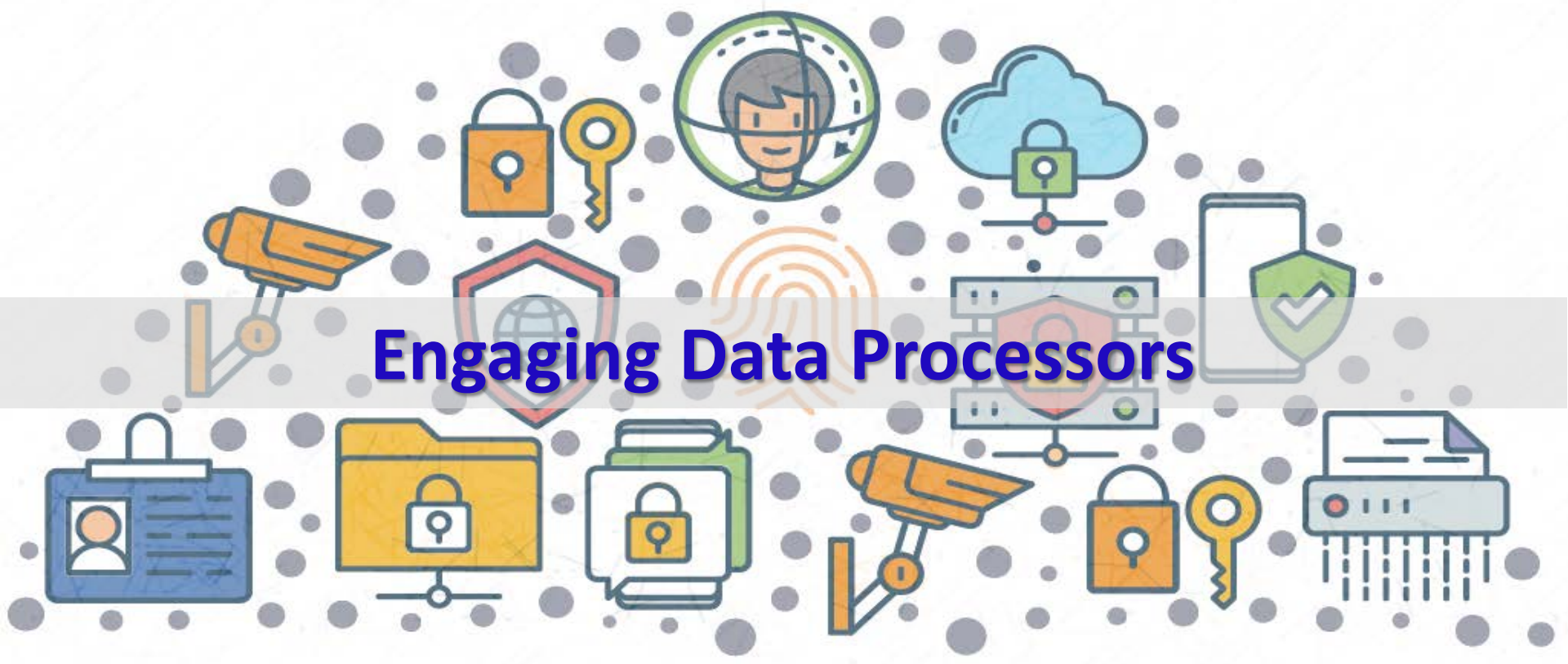
BACKGROUND

- 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.



Engaging Data Processors

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)]*

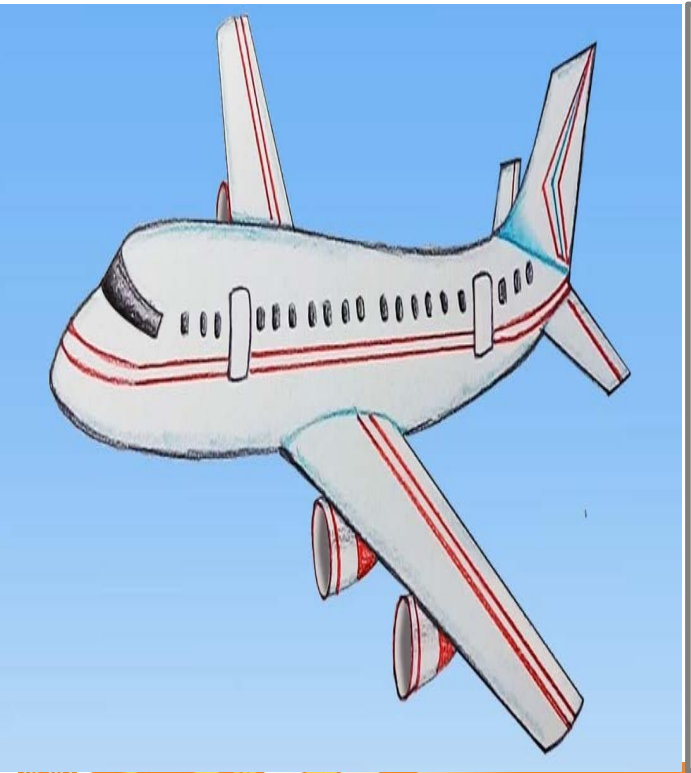
What to pay attention to when picking a cloud service provider (CSP)?

- Ensure an **equivalent level of protection of personal data** like any other type of computing model when in a cloud computing environment.
- Consider the **locations of data centers**.
- Obtain **sufficient assurance** from CSP on technical and organisational data protection measures, for example:
  - Have data protection and IT security **certifications** by accredited third parties (e.g ISO 27001, ISO 27701);
  - Adhere to **cloud-specific codes of conduct** in terms of measures protecting personal data in a cloud-specific environment;
  - Have **previous experience** on projects also handling health data; and
  - **Accountability practices** are in place, such as Data Protection Officer, robust privacy policies and procedures, privacy impact assessments, auditing and assessment practices, etc.
- Data users may make reference to *"**ISO/IEC 27018,** a Code of practice for personally identifiable information (PII) protection in public clouds acting as PII processors*" for cloud-specific privacy controls.

Source: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-use-cloud-computing-services-european_en

Data Breach Incidents

Data Breach Incident (1)



Cathay Pacific -- Data breach incident of unauthorised access to personal data of approximately 9.4 million passengers

PCPD: Failed to take all reasonably practicable steps to protect the affected passengers' personal data against unauthorised access in terms of ***vulnerability management***, ***adoption of effective technical security measures*** and ***data governance***

Data Breach Incident (1)

Low risk alertness

Corporate governance failure

Risk assessment failure

Vulnerability scanning exercise at a yearly interval (too lax)

Risk assessment failure

Failure to identify and address the commonly known exploitable vulnerability

Operational measure failure

Failure to have an effective personal data inventory

Failure to apply effective multi-factor authentication to all remote users

Technical measure failure

Data Breach Incident (2)

Hong Kong Broadband Network Limited

- Inactive database was intruded that caused leakage of personal data of about 380,000 customers and service applicants

PCPD:

- Insufficient safeguards for the database
- Failure to exercise control over the IT and security facilities for the personal data of customers
- Leading to a data breach which could have been avoided

Data Breach Incident (3)

選舉事務處亞博館遺失手提電腦　內載全港選民資料恐爆私隱災難

社會新聞

Registration and Electoral Office – Loss of two notebook computers containing personal data of 1,200 Election Committee members and 3.78 million Geographical Constituencies electors in 2017

PCPD:

- Security measures not proportional to the degree of sensitivity of the data and the harm that might result from a security incident
- Lacked the requisite awareness and vigilance as expected

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

Proposed PDPO Amendments

Data breach of an airline based in Hong Kong affecting 9.4m passengers

- Suspicious activities on its network detected in March 2018
- Data breach notification not lodged to PCPD until 24 Oct 2018
- 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

Call for amendment of PDPO

The Government presented amendment directions for the PDPO to Legislative Council in January 2020:

I. Mandatory data breach notification mechanism
II. Requirements on setting out data retention policy
III. Increasing PCPD's sanctioning powers
IV. Regulating data processors directly
V. Clarifying the definition of 'personal data'
VI. Regulation of doxxing

Existing Issues

(I) Mandatory Breach Notification Mechanism

Leakage of personal data on the internet is common in information age

Number of data breaches in Hong Kong has been increasing steadily in recent years

No. of data breach notifications received by PCPD **reached a record-high of 139 in 2019**, almost double that in 2014

Existing Issues

(I) Mandatory Breach Notification Mechanism

Some data users **took months to voluntarily report a data breach**, falling short of society's expectations

Prompt notifications are important for **mitigating measures** to be taken to prevent further damage

The **global data protection landscape** has moved towards a mandatory breach notification regime

Possible Amendments

(I) Mandatory Breach Notification Mechanism

- Notify both the **PCPD** and the **impacted individuals**
- Notification threshold – "***real risk of significant harm***"
- Set **time limit** – e.g. 5 business days for notifying PCPD
- May allow for investigation period for 'suspected breach' before notification (e.g. 30 days)
- PCPD may direct data user to notify impacted individuals
- Failure to make notification may result in administrative fine imposed by PCPD.

Existing Issues

(II) Additional regulation on retention of personal data

Current provisions:

Data Protection Principle 2:

Personal data is **not kept longer than is necessary** for the fulfilment of the purpose for which the data is or is to be used

Does not define when personal data is "no longer necessary"

No fixed retention period requirements

No requirements for setting data retention policy

But there is no one-size-fit-all approach to data retention

Possible Amendments

(II) Additional regulation on the retention of personal data

- Amend DPP5(a) to expressly include the retention policy in the information to be made available
- Data users to formulate and disclose personal data **retention policy**
- Disclose **maximum retention** period for different categories of personal data

(III) PCPD's Sanctioning Powers

Existing Issues

PCPD has no authority to impose administrative fines, or carry out criminal investigation and prosecution

Current penalty provisions in the PDPO:

- Contravention of DPPs is not an offence
- PCPD may issue an enforcement notice, non-compliance with which is a criminal offence
- Offences under S.64 (e.g. criminal doxxing) and Part 6A (direct marketing) may attract higher penalties

Penalty levels may not reflect the seriousness of the offence and the harm suffered by affected data subjects:

- From 1996 to June 2020: only 35 cases resulted in conviction by court (mostly direct marketing-related), fines imposed were all relatively low

PDPO criticised for its weak deterrent effect

Possible Amendments

(III) PCPD's Sanctioning Powers

- Confer additional powers on the PCPD to impose **administrative fines**
- Maximum level of fine may be a **fixed amount or a percentage of the annual turnover**, whichever is higher
- Administrative fines **credited to the HKSAR Government** and not the coffers of the PCPD

(IV) Regulate data processors directly

Existing Issues

Outsourcing data activities are becoming more common

The PDPO does not regulate data processors

- Data processor acting purely on behalf of an overseas data user is not subjected to regulatory oversight of PDPO, i,e, PCPD cannot investigate breaches of DPPs.
- The apportionment of responsibility between data users and data processors is often unclear, resulting in insufficient data protection
- Hong Kong's reputation as a regional or international data centre is compromised if the PCPD has no *locus standi* to investigate data security incidents involving processors (e.g. cloud service providers)

(IV) Regulate data processors directly

Direct regulation of data processors can…

- Eliminate legal loopholes in existing provisions
- Ensure **fair share of responsibilities** between data users and data processors
- Enhance protection for personal data during processing

Improve the cloud readiness and reputation of Hong Kong by attaining a **satisfactory regulatory environment**

Possible Amendments

(IV) Regulate data processors directly

Data processors' obligations on:

- **retention period** of personal data
- **security** of personal data
- **notification to data users and PCPD** of data breaches without undue delay


Data Ethics

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

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

Accountability & Ethics as a Bridge between Law and Expectation

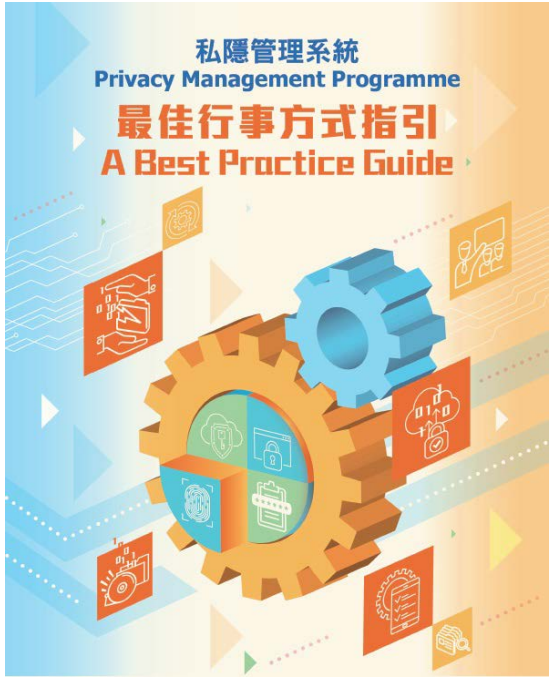
LEGISLATION

PUBLIC EXPECTATION

Technology development

Vast amount of data collected & processed

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



Download >>

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

Data Ethics

Privacy Management Programme

Extended obligation to ensure compliance with laws

Personal Data (Privacy) Ordinance

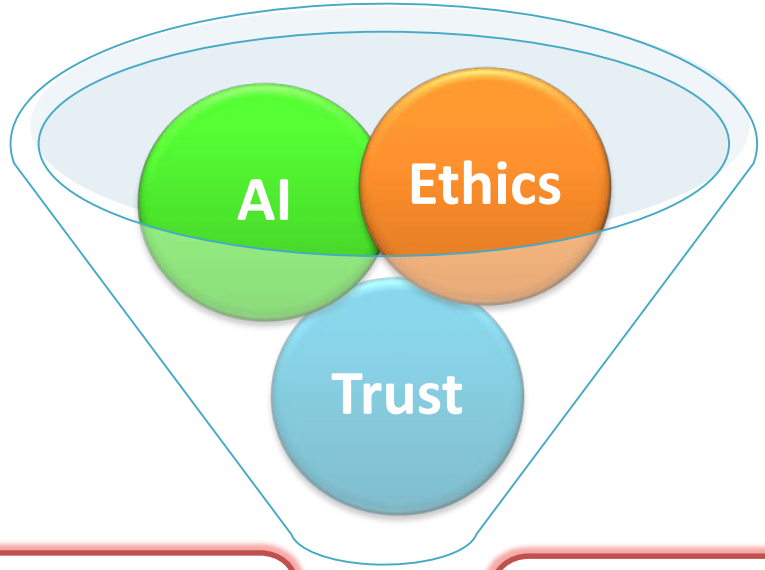
Legal obligations

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

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

3 Core Values of Data Ethics

Benefits



Improved reputation & trustworthiness

Individuals more willing to share data

Sharpening competitive edges

Security Issues in relation to privacy arising from COVID-19

1. Zoom's Privacy and Security Issues

- It is reported by media that Zoom had transferred certain data of users using iOS mobile apps to Facebook
- Allow meeting hosts to track attendees
- 'Zoombombing' : uninvited guests join video conferences, usually to shout abuse, share pornography or make racist remarks

PCPD Media Statement on
Zoom Data Security Incident dated 1 April 2020:

PCPD Publication:
“13 Privacy Tips for Online Video-conferencing”

For Conference Hosts

Before online teaching / video-conferencing

1. **Take security measures**
   Install the latest version of the programme, anti-virus software and firewalls; conduct privacy impact assessment
2. **Guard the gate**
   As a “gatekeeper”, use the virtual “Waiting Room” to conduct “mandatory quarantine” to verify the participants’ identity before the meeting so as to prevent “gate crashing” or “bombing”
3. **Manage meeting ID and password**
   Design a meeting ID and password specifically for the teaching / meeting; do not re-use the password; send the password separately to participants only
4. **Don’t use public Wi-Fi**
   Set encryption for Wi-Fi network

During online teaching / video-conferencing

5. **No unauthorised admission**
   Select the “Lock Meeting” function to bar strangers from joining the meeting
6. **Be in control**
   Only the teacher and the host can share the screen; allow screen sharing on a need basis only
7. **Video or audio recording only when necessary**
   Disable recording; if recording is necessary, notify participants beforehand
8. **Mind participants’ activities**
   Monitor content shared by participants; remove inappropriate information and unidentified persons

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

PCPD publication:
“13 Privacy Tips for Online Video-conferencing”

Download >>

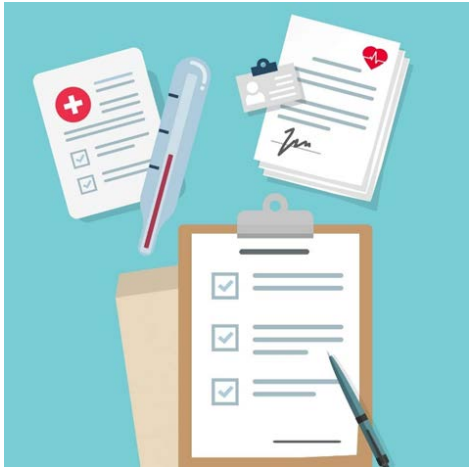
PCPD.org.hk
香港個人資料私隱專員公署
Privacy Commissioner for Personal Data, Hong Kong

2. Security of Personal Data Collected for Combatting COVID-19

- any measures that may intrude personal data privacy should be necessary, appropriate and proportionate
- organisations as data users must comply with the PDPO and seek to process the relevant data in an anonymised or de-identified way
- least privacy-intrusive measures should be preferred

2. Security of Personal Data Collected for Combatting COVID-19

- Organisations are required to take all practicable steps (such as providing a Personal Information Collection Statement (PICS)) on or before data collection to inform individuals of the type of personal data to be collected and the purposes (e.g. protection of public health), and the classes of persons (e.g. public health authorities) to whom their data may be transferred, etc.
- It is also a good practice to inform the individuals through the PICS the maximum period of time for which the data will be retained.



2. Security of Personal Data Collected for Combatting COVID-19

- organisations shall permanently destroy the personal data collected for the purposes of combatting COVID-19 when the purpose of collection is fulfilled, such as when there is no evidence suggesting that any visitors have contracted COVID-19 or have close contacts with the infected after a reasonable period of time.
- all practicable steps (e.g. storing the data in a locked cabinet, encrypting the data and only allowing authorised personnel to have access to the data) shall be taken to protect the personal data
- adequate data security safeguards are particularly important for medical or health data

3. Security Measures while Work from Home

Before transferring paper or digital files from work to home:

- Encrypt digital data
- Seek approval from supervisor
- Minimise transfer of data
- Body-weld documents or devices during transportation
- Redact personal data / confidential information
- Keep proper logs on movement of data

3. Security Measures while Work from Home

Security advice for homeworking employees who are using their own devices:

- Use Multi-Factor Authentication
- Authenticate participants in online meetings before start
- Never share work device's account with others
- Install proper anti-virus software
- Ensure Wi-Fi connection is secure
- Perform regular system updates for the devices

Guidelines Issued by the Privacy Commissioner on Privacy Issues arising from COVID-19

- Fight COVID-19 Pandemic: Privacy Commissioner Provides Advisory to Premises Operators on Temperature Measurement and Collection of Relevant Personal Data dated 27 July 2020
- Fight COVID-19 Pandemic: Guidelines for Employers and Employees dated 30 March 2020
- Response to media enquiry on privacy issues arising from COVID-19 dated 21 March 2020
- The use of information on social media for tracking potential carriers of COVID-19 dated 26 February 2020
- Privacy issues arising from mandatory quarantine measures dated 12 February 2020

Download >>

Contact Us

Hotline	2827 2827
Fax	2877 7026
E-mail	communications@pcpd.org.hk
Website	www.pcpd.org.hk
Address	Room 1303, 13/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong

"Privacy in Sunlight" Reaching out through Instagram, LinkedIn, Twitter, Weibo, Facebook and YouTube

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