Protection of Personal Data and Cyber Security Challenges in Healthcare Sector

8 October 2021

Disclaimer:

The information provided in this PowerPoint is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (PDPO). For a complete and definitive statement of law, direct reference should be made to the PDPO itself. The Privacy Commissioner for Personal Data makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information set out in this PowerPoint. The contents provided will not affect the exercise of the functions and powers conferred to the Privacy Commissioner for Personal Data under the PDPO.

What is 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 (Privacy) Ordinance, Chapter 486 (PDPO)
6 Data Protection Principles (DPPs)

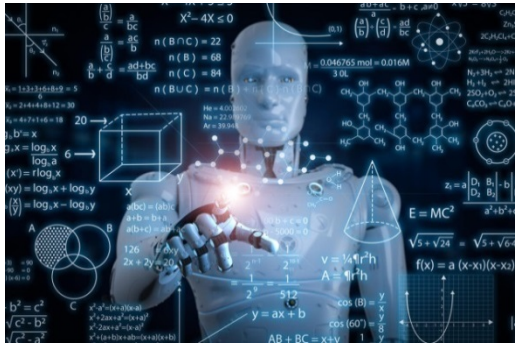
- Represent the core requirements of the PDPO
- Cover the entire lifecycle of personal data from collection, holding, processing, use to deletion
- Data users have to comply with the DPPs

Source: [Asia Pacific Privacy Authorities]

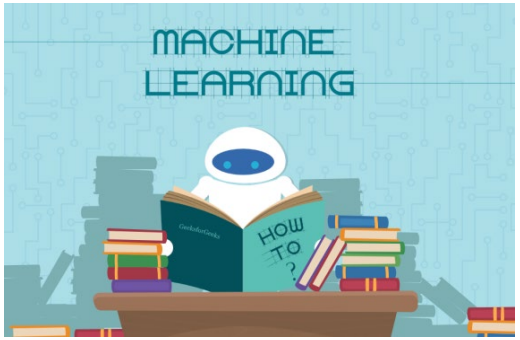
Definition of Personal Data - expanding

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

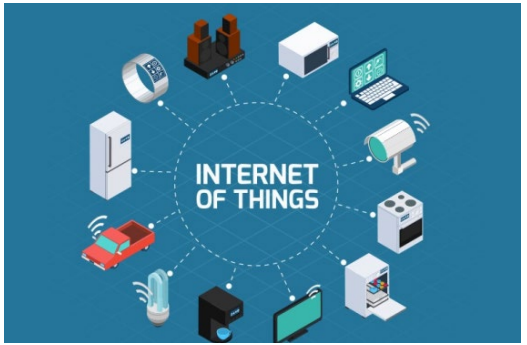
Advancement in Technology



Robotics



Machine learning



Internet of Things

Artificial Intelligence

Autonomous vehicles

Big Data


Contact addresses and details
Identifiers
PASSPORT
Contacts and accounts
Relationships
Support history
Call centre logs
Unstructured documents
Email text and sentiment
Social media sentiment
Order history

Data is the Lifeblood of a Data-driven Economy

1

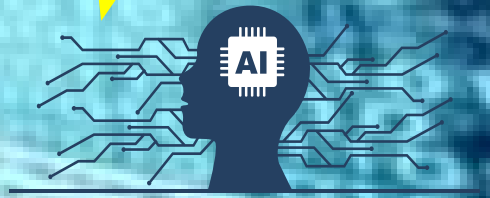
Collection of big data from various sources

2

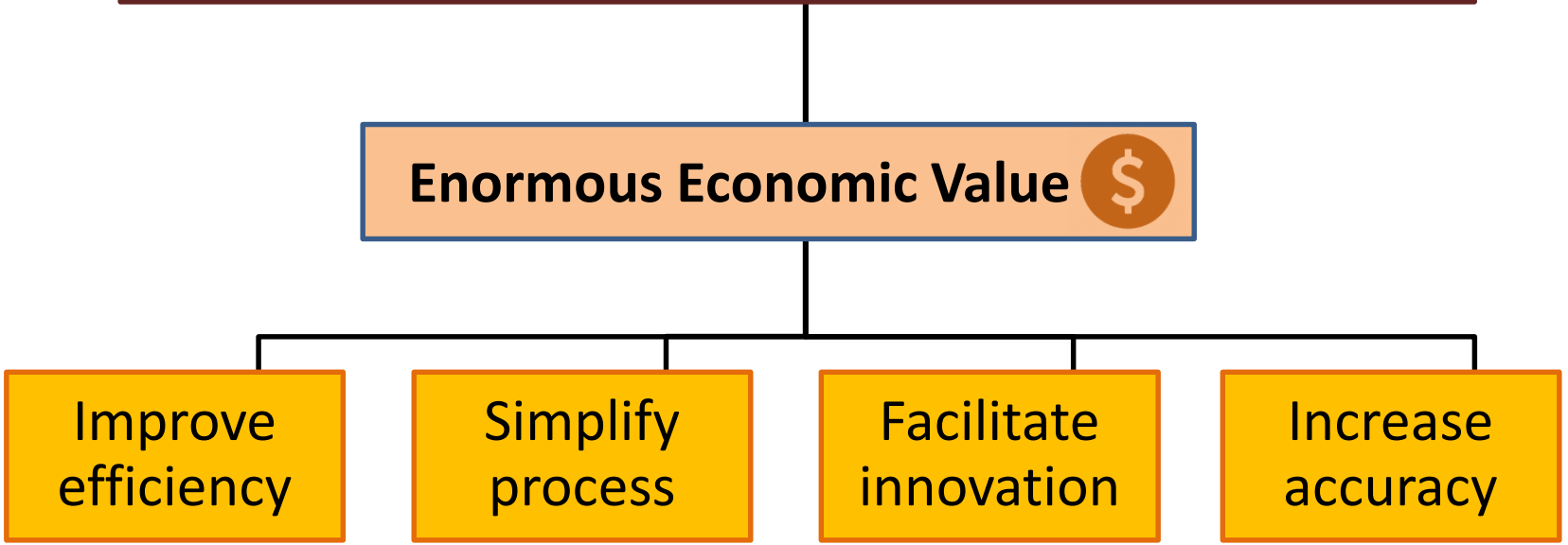
Data analytics by AI

3

Automated decision making & improvement in business processes and services

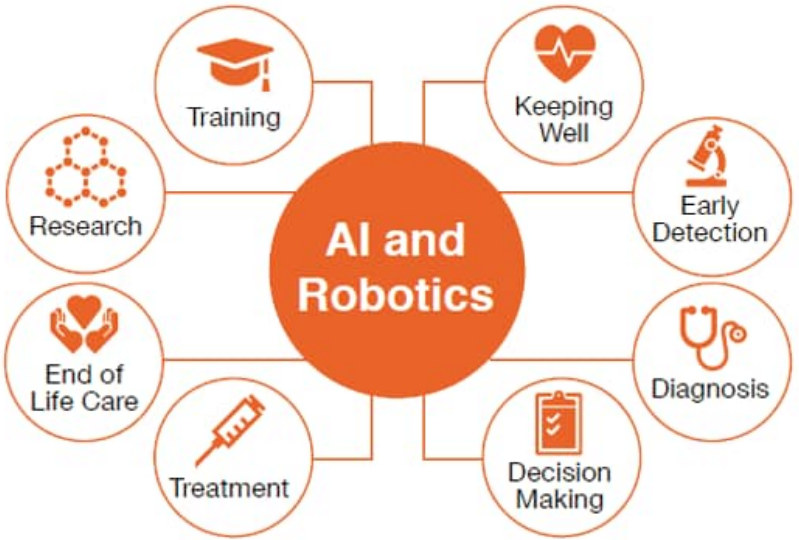


Positive Impacts of AI & Big Data



Application of AI in Healthcare

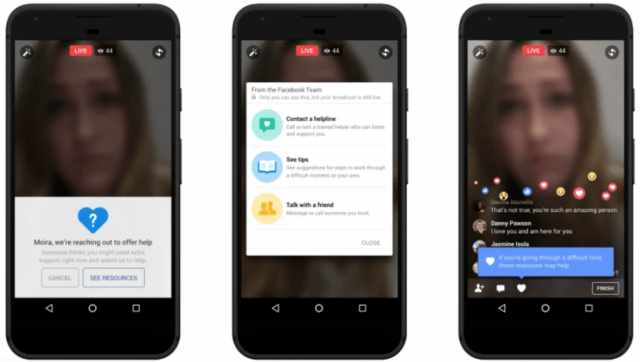
- Enhance Primary Care and Triage
- Support in Clinical Decisions
- Robotic Surgeries
- Virtual nursing assistants
- Aiding in the accurate diagnosis

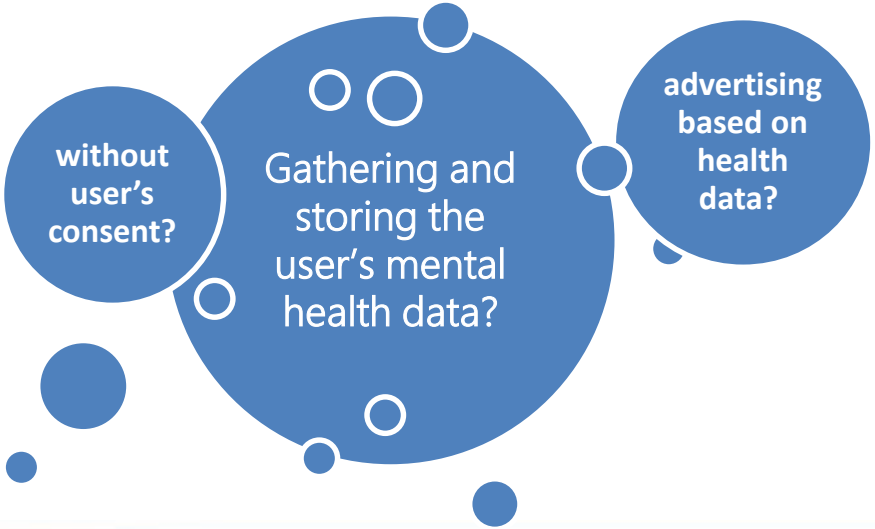


Source: https://www.analyticssteps.com/blogs/artificial-intelligence-healthcare-applications-and-threats;
https://www.pwc.com/gx/en/industries/healthcare/publications/ai-robotics-new-health/transforming-healthcare.html

Application of AI in Healthcare

In late 2017, a social media platform rolled out a "**suicide detection algorithm**" in an effort to promote suicide awareness and prevention. The system uses AI to gather data from the user's posts and then predict his mental state and propensity to commit suicide.





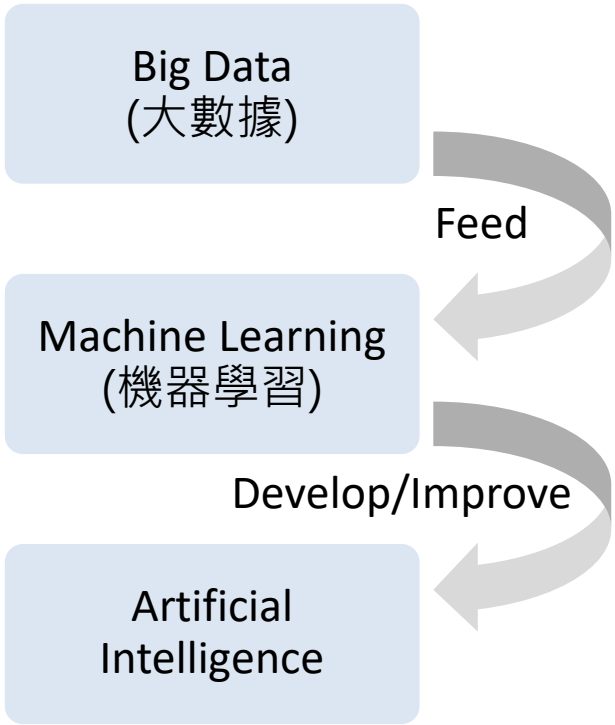
Source: https://www.lexalytics.com/lexablog/ai-healthcare-data-privacy-ethics-issues
https://techcrunch.com/2017/11/27/facebook-ai-suicide-prevention/

Privacy Concerns of Using AI in Healthcare

- Collection of huge datasets
- Access, use and control of patient data
- Storage and data security
- Exchange of data between health systems and AI developers
- Problem of reidentification
- Capability of predicting private information

Source: https://www.analyticssteps.com/blogs/artificial-intelligence-healthcare-applications-and-threats#google_vignette
https://www.lexalytics.com/lexablog/ai-healthcare-data-privacy-ethics-issues
https://bmcmedethics.biomedcentral.com/articles/10.1186/s12910-021-00687-3

Impacts of AI on Data Privacy



Possible Impacts on Privacy

1) Excessive Collection & Retention of Data
2) Lack of Transparency
3) Unpredictable Use
4) Bias and Discrimination
5) Re-identification

Challenges to Data Protection Principles

“Guidance on the Ethical Development and Use of Artificial Intelligence”

OBJECTIVES

1. To provide guidance to enable organisations to develop and use AI in compliance with the requirements under the PDPO and in an ethical manner
2. To facilitate healthy development and use of AI in Hong Kong
3. To facilitate Hong Kong to become an innovation and technology hub (創科中心) and world-class smart city (智慧城市)

Guidance on the Ethical Development and Use of

Artificial Intelligence

PCPD.org.hk

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

Download

Ethical AI

3 Three Data Stewardship Values

- Being Respectful
- Being Beneficial
- Being Fair

7 Seven Ethical Principles for AI

- Accountability
- Human Oversight
- Transparency and Interpretability
- Data Privacy
- Fairness
- Beneficial AI
- Reliability, Robustness and Security

4 Four Major Business Processes

- AI Strategy and Governance
- Risk Assessment and Human Oversight
- Development of AI Models and Management of AI Systems
- Communication and Engagement with Stakeholders

How much is your data worth?

Category	Price (USD)
Cloned VISA with PIN	$25
Credit Card details, account balance up to $1,000	$150
Credit Card details, account balance up to $5,000	$240
Stolen online banking logins, minimum $100 on account	$40
Stolen online banking logins, minimum $2,000 on account	$120
Stolen PayPal account details, minimum $1000 on account	$120
Hacked Facebook account	$65
Hacked Instagram account	$45
Hacked Gmail account	$80
Uber driver hacked account	$14
Netflix account – 1 year subscription	$44

Source: https://www.privacyaffairs.com/dark-web-price-index-2021/

How about medical data?

- Medical records contain a treasure trove of unalterable data points, such as a patient's medical and behavioral health history and demographics, as well as their health insurance and contact information.
- Cybercrime organizations can sell stolen medical records for as much as $1,000 each.
- Patients of a large mental and behavioral health practice in Finland this year were blackmailed by a hacker. Patients received extortion letters from the cybercriminals demanding as much $240 to keep their information private.
- Medical identity theft, which is where a patient's identity is fraudulently used to obtain medical services or prescriptions, costs $13,500 to resolve.
- One of the newer trends is stealing the identities of doctors (selling on the dark web for $500).

Source: https://capsuletech.com/blog/stolen-patient-records-a-hot-commodity-on-the-dark-web
https://www.totalprocessing.com/totalprocessing.com/public/blog/how-much-is-your-data-worth-on-the-dark-web

DPP4 - 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”?

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…

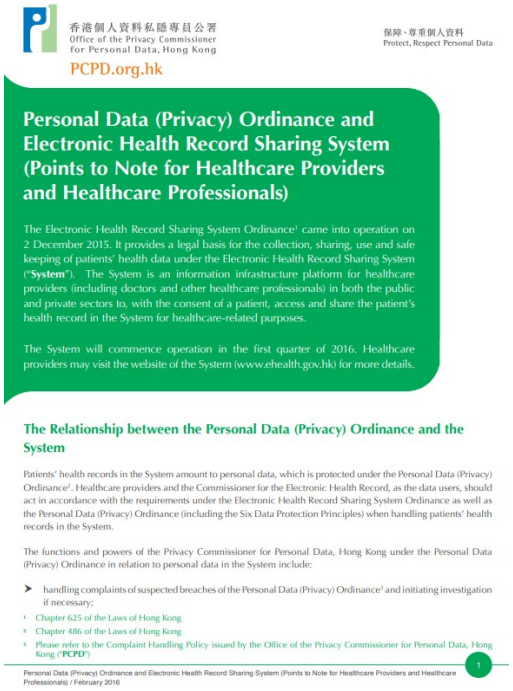
CASE 3

- 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



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

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

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**").

Download

Download

What is a Data Breach?

- A suspected breach of security of personal data held by a data user, which results in exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use.
- The breach may amount to a contravention of Data Protection Principle 4 – Security of personal data.
- PCPD has always encouraged data users to give data breach notifications to affected individuals and PCPD to minimise the potential damage which might be caused to individuals.

Data Breach Is on the Rise:
Major data breaches in recent years and individuals affected

2020	Estée Lauder	440 million
	Microsoft	250 million
	Instagram, TikTok, Youtube	235 million
2019	Capital One (Bank)	160 million
	Zynga (Online game developer)	218 million
	Facebook	419 million
2018	Marriott Hotel	383 million
	Twitter	330 million
	Facebook	140 million
	Uber	57 million
	Cathay Pacific Airways	9.4 million

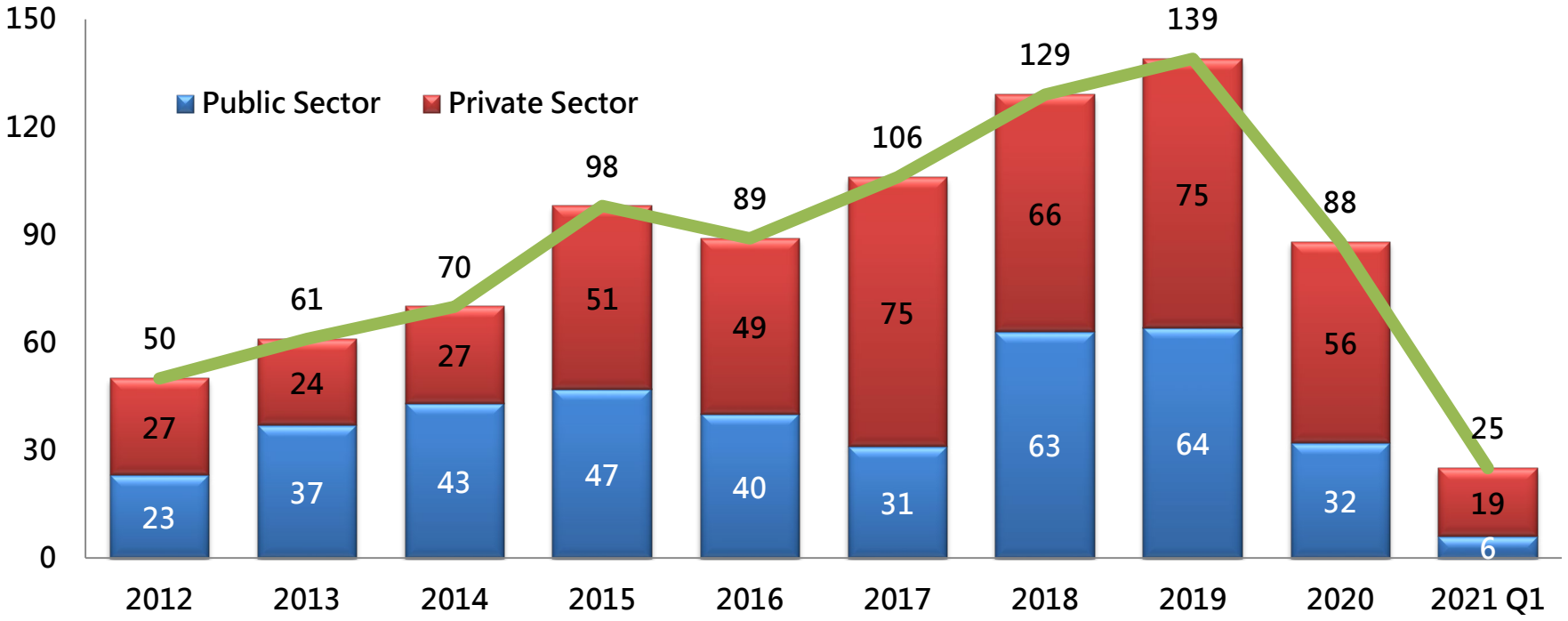
Reference: Nord VPN, Forbes

Major data breaches in 2021

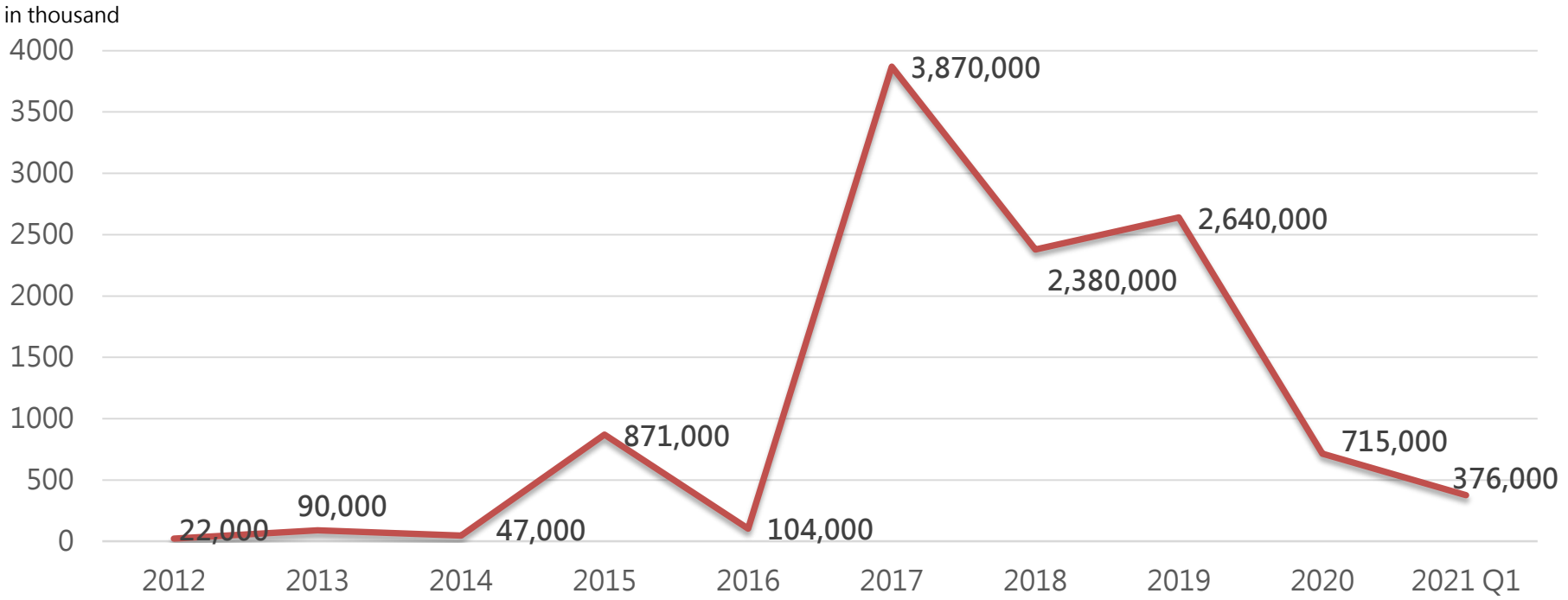
Platforms	Affected individuals	Individuals in Hong Kong
Facebook	533 million	2.93 million
LinkedIn	500 million	280,000 (All Hong Kong users)
Clubhouse	1.3 million	Unknown
Air India	4.5 million	Unknown

Over
1 billion
users affected

Numbers of Data Breach Notifications Received by PCPD



Numbers of Affected Individuals in Hong Kong



Recommended Practice for Handling Data Breach

- Collect essential information immediately
- Assess the impact on data subjects
- Adopt containment measures
- Contact stakeholders (e.g. services provider, management and affected data subjects)
- Consider giving data breach notification to PCPD

Data Breach Notification Form

- Details about the data breach
- Types of personal data involved
- Number of affected data subjects
- Risk of harm
- Containment actions

To: Privacy Commissioner for Personal Data, Hong Kong

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

Data Breach Notification Form

Notice

Notification of a data breach to the Privacy Commissioner for Personal Data, Hong Kong (the **"Commissioner"**) by the data user *(see Note 1)* is not a legal requirement. In deciding whether or not to give this notification to the Commissioner, you should consider the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Commissioner. In most cases, it is advisable to give notifications to the data subject(s) *(see Note 2)* affected by the breach.

PARTICULARS OF THE PERSON GIVING THIS NOTIFICATION (i.e. the data user)

Name:

Address:

Telephone number: Fax number:

Email address:

Where the person giving this notification is an organization, please provide the following information:

Contact person :

Name (*Mr./Ms./Miss):

Relationship with the Reporting Organization (e.g. job title):

Telephone number: Fax number:

Email address:

(*Please delete as appropriate)

DETAILS ABOUT THE DATA BREACH *(see Note 3)*:

Publications

Download >>

Common Causes of Data Breach

Loss of documents or portable storage devices

(34%)

Hacking / System misconfiguration

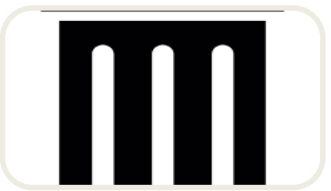
(32%)

Inadvertent disclosure through mail/email

(21%)

Employee misconduct

(10%)



Improper / Accidental disposal

(3%)

Cyber Attack

Network-attached storage servers of a university were hacked

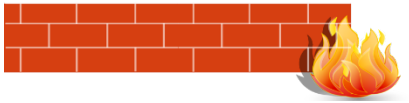
BACKGROUND

- 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

Cyber Attack



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

Compliance Investigations: (1) Intrusion into customer database

Background

An obsolete database (inactive for 6 years) owned by a broadband network company was intruded in 2018 that caused leakage of personal data of about 380,000 customers

Result of Investigation

- Contravened Data Protection Principle 2(2) & 4(1) – retention & security of personal data
- Failed to conduct a comprehensive and prudent review after system migration
- Failed to give due consideration to the retention period of former customers' personal data
- Issued an Enforcement Notice – to devise clear procedures for system migration and data retention and security policies; and to erase personal data retained longer than necessary

Compliance Investigations: (2) Unauthorised access to credit reports

Background

A local newspaper passed through the online authentication procedures of a credit reference agency and obtained the credit reports of a number of public figures

Result of Investigation

- Contravened Data Protection Principle 4(1) - security of personal data
- Vulnerabilities in online identity authentication process
- Issued an Enforcement Notice – to undergo one-time password verifications for online credit report applications; and to devise clear procedures to ensure that the Q&A for knowledge-based authentications are relevant, functional and up-to-date

Risks of Engaging Data Processors

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

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

"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

Lesson Learnt to Prevent Recurrence

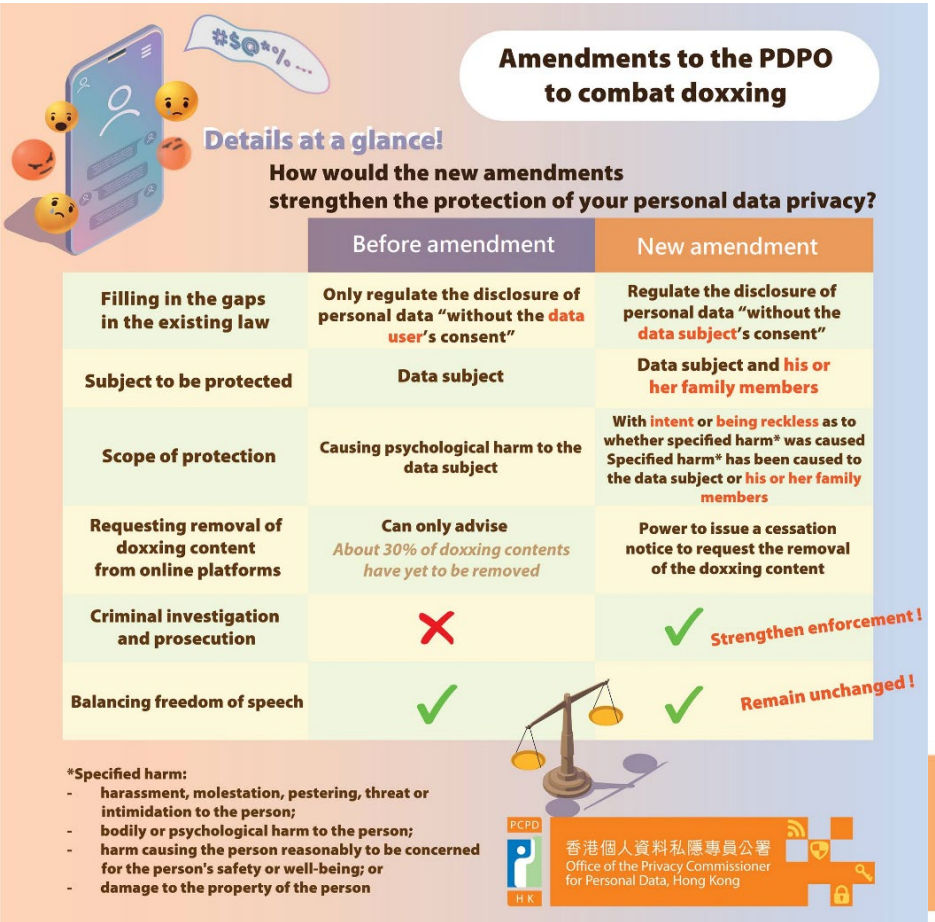
- improvement of security
- control of access rights
- revision or promulgation of privacy policy and practice
- effective detection of data breach
- strengthening of monitoring and supervision
- provision of on-the-job training

LESSON LEARNT

Offences

- Contravention of DPP is not an offence. The Commissioner may serve an enforcement notice on the relevant data user directing the data user to remedy the contravention.
- Non-compliance with an enforcement notice commits an offence and carries a penalty of a fine at $50,000 and imprisonment of 2 years.
- Repeated non-compliance with enforcement notice carries a penalty of a fine at $100,000 and imprisonment of 2 years, in case of a continuing offence, a daily fine of $2,000
- Same infringement of the second time commits an offence and carries a penalty of a fine at $50,000 and imprisonment of 2 years

Offences under section 64 of PDPO



Personal Data (Privacy) (Amendment) Ordinance 2021

- Comes into effect on 8 October 2021
- Please visit our website for more information: www.pcpd.org.hk

Contact Us

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