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

Data Security, Cybersecurity and AI Security: the Privacy Commissioner’s Perspective

Law Lectures for Practitioners 2024

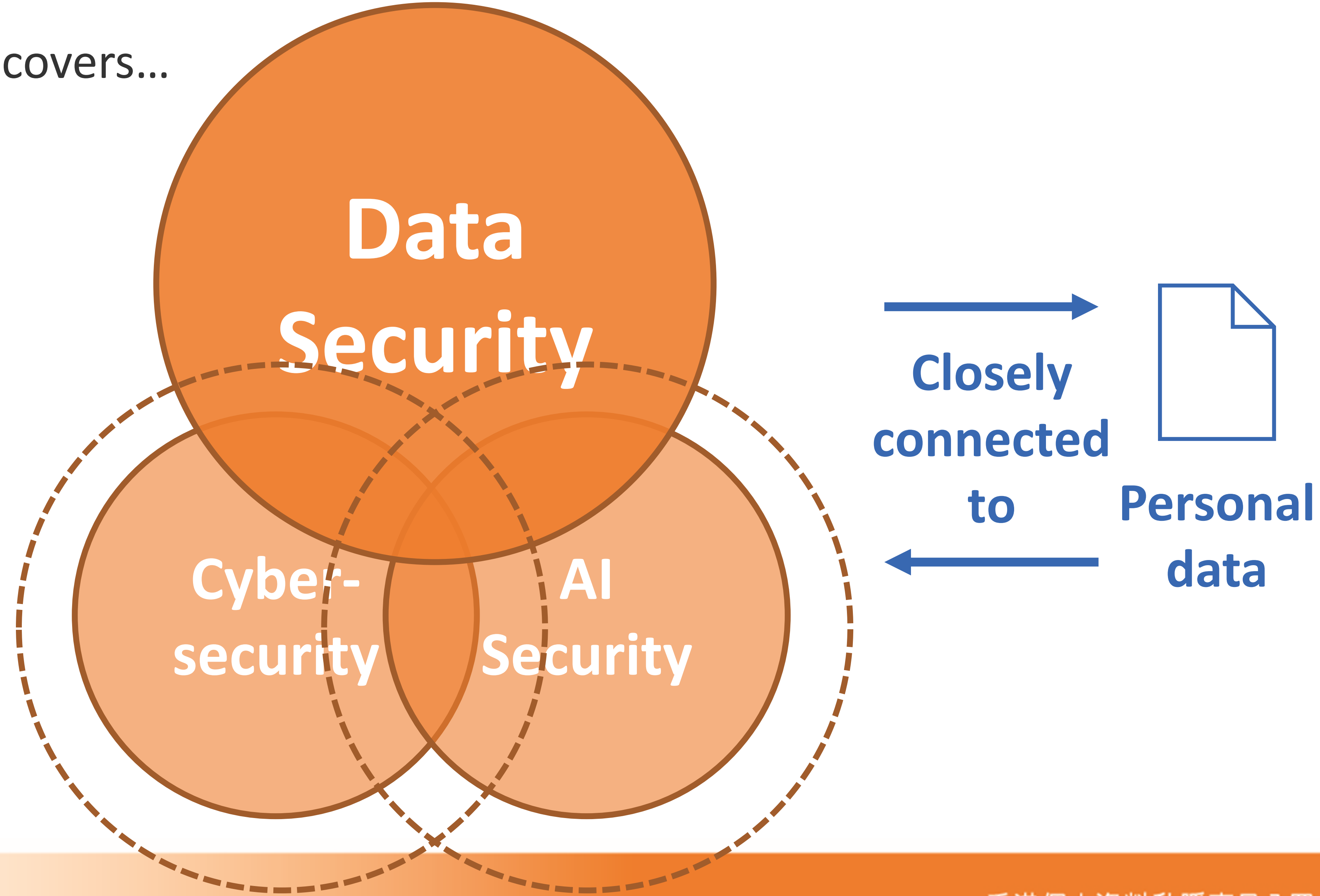
The University of Hong Kong

17 October 2024

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data

Content

This presentation covers...



Definition

Personal data means any data –

(Section 2(1) of the PDPO)

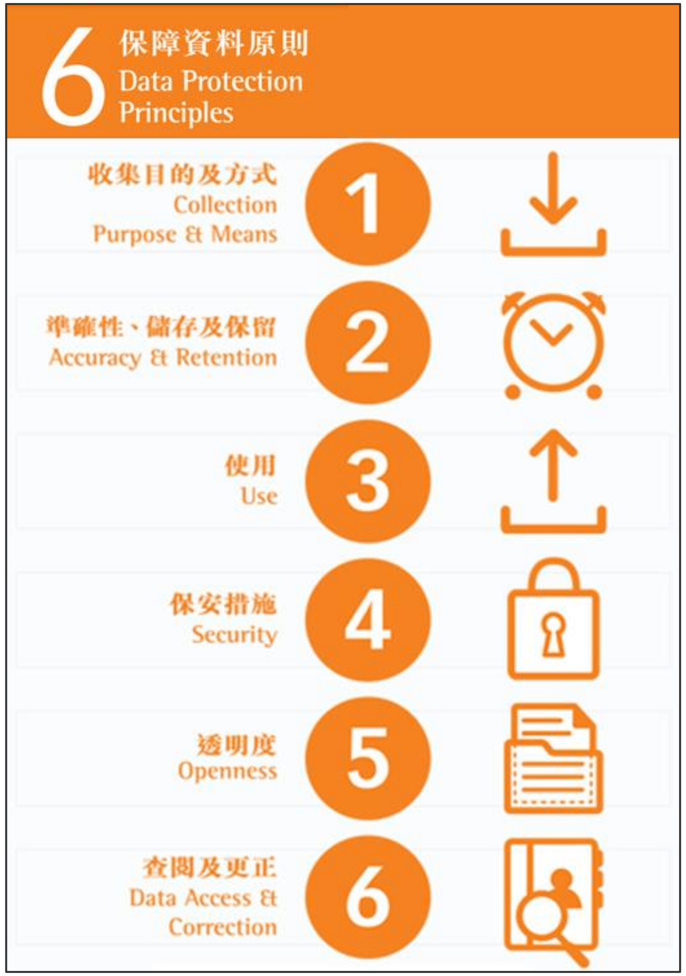
Relating directly or indirectly to a living **individual**;

From which it is practicable for the **identity** of the individual to be directly or indirectly **ascertained**; and

In a form in which **access to or processing of** the data is **practicable**

6 Data Protection Principles

(Schedule 1 to the PDPO)



6 保障資料原則 Data Protection Principles

1 收集目的及方式 Collection Purpose & Means

2 準確性、儲存及保留 Accuracy & Retention

3 使用 Use

4 保安措施 Security

5 透明度 Openness

6 查閱及更正 Data Access & Correction

Represent the core requirements of the **Personal Data (Privacy) Ordinance (PDPO)**

Cover the **entire lifecycle** of the handling of personal data, from **collection, holding, processing, use to deletion**

Data users must comply with the DPPs

Legal Liability
Security of personal data

DPP4(1)

A data user shall take **all reasonably practicable steps** to ensure that the personal data it holds is protected against unauthorised or accidental access, processing, erasure, loss or use.

DPP4(2)

If 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 unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

Content

We now turn to…

Data Security

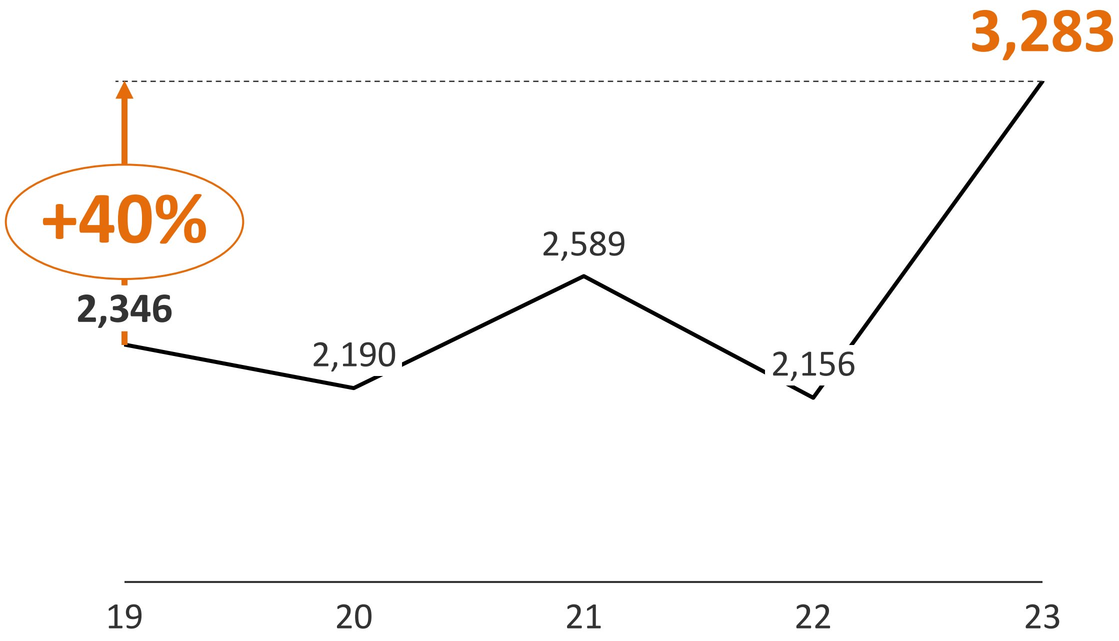
Global Situation

Cyberattacks are rising

📊 Data breach incidents in the cyber world have risen

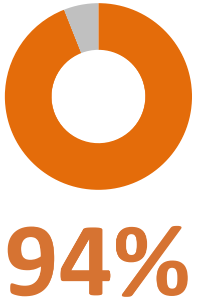
Cyber personal data breach incidents

UK, 2019 – 2023

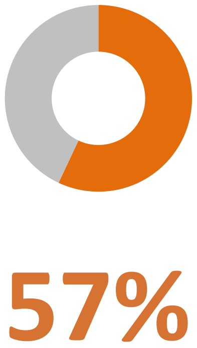


Source: ICO

🛌 The prevalence of cyberattacks leave IT professionals sleepless



of **organisations** experienced **cyberattacks** in a global survey



of **IT professionals lost sleep** worrying about their organisations being hit by a cyberattack

Source: Sophos

Global Situation

Two incidents indicate the grave consequences of cyberattacks

Casino giant MGM expects $100 million hit from hack that led to data breach

By Zeba Siddiqui

October 6, 2023 10:35 AM GMT+8 · Updated a year ago

The MGM case (2023)

- Hackers used **vishing (voice phishing)** and **other techniques** to get access to MGM's systems. They then used ransomware to encrypt MGM's data
- Data of customers that used MGM services before 2019, such as **contact information, date of birth and driver's licence numbers**, were leaked
- Took 10 days for MGM to announce that its hotels and casinos resumed operating normally
- **Costs** from the incident **exceeded US$110 million**

Source: Reuters (2023); Security Week (2023); Vox (2023); Z Cybersecurity

Medibank says hacker accessed data of 9.7 million customers, refuses to pay ransom

Reuters

November 8, 2022 5:05 AM GMT+8 · Updated a year ago

The Medibank case (2022)

- Hackers used the **credential stolen** from an account to gain preferential access to the internal system of the insurer, resulting in the **health data of over 9 million customers released on the dark web**
- Australian Information Commissioner filed civil penalty proceedings against Medibank in June 2024 for **failing to take reasonable steps to protect Australians' personal data from misuse and unauthorised access or disclosure**

Source: Reuters (2022), OAIC (2024)

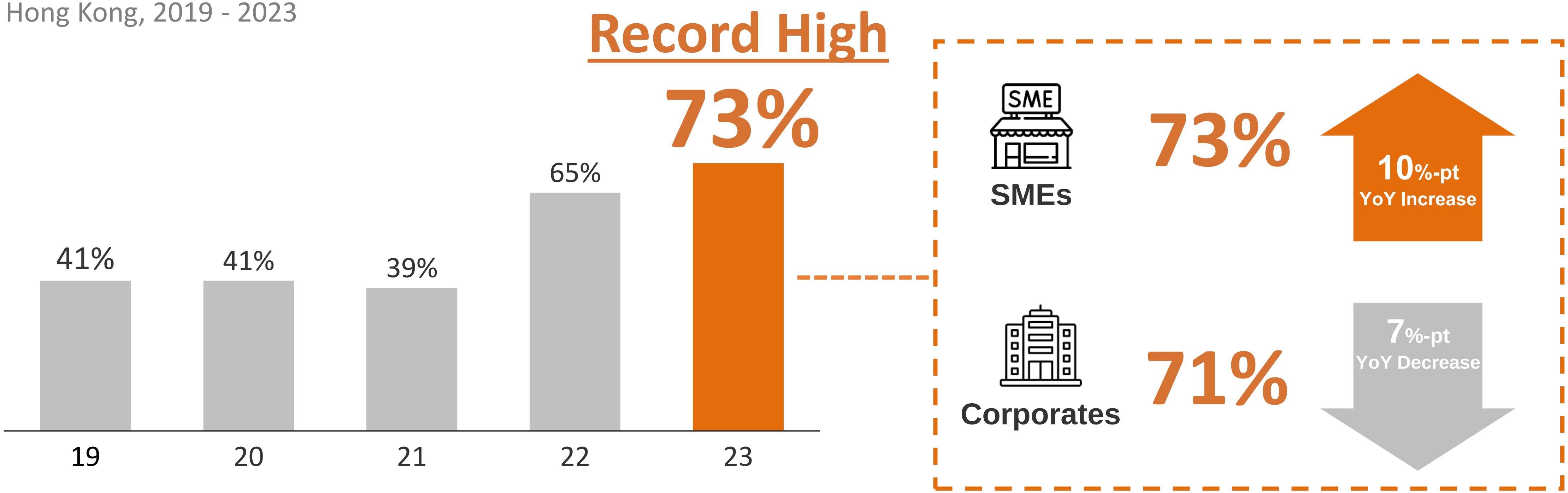
Local Cyber Attacks

Cyberattacks are also increasing in Hong Kong

📈 **PCPD's survey with HKPC shows nearly ¾ of enterprises faced cyberattacks in 2023, the highest in five years**

% of enterprises that encountered cyberattacks in the past 12 months

Hong Kong, 2019 - 2023



SMEs 73% 10%-pt YoY Increase

Corporates 71% 7%-pt YoY Decrease

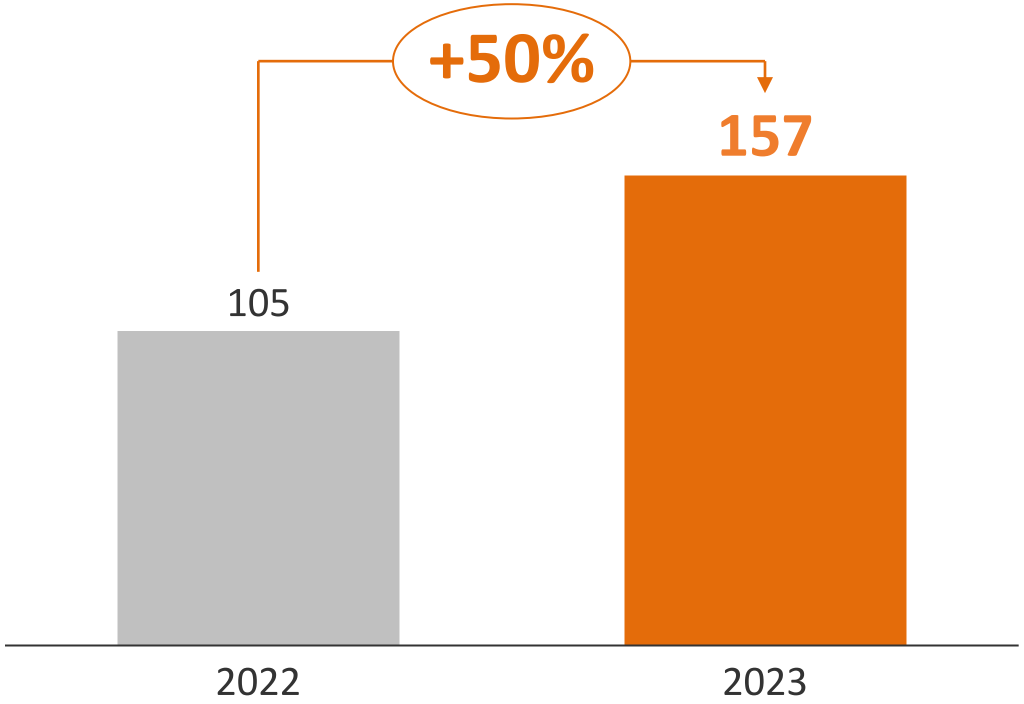
Source: Hong Kong Enterprise Cyber Security Readiness Index

Local Data Breaches

Data breach notifications rose in 2023; hacking was a major contributor

Compared to 2022, DBNs in 2023 rose substantially by 50%

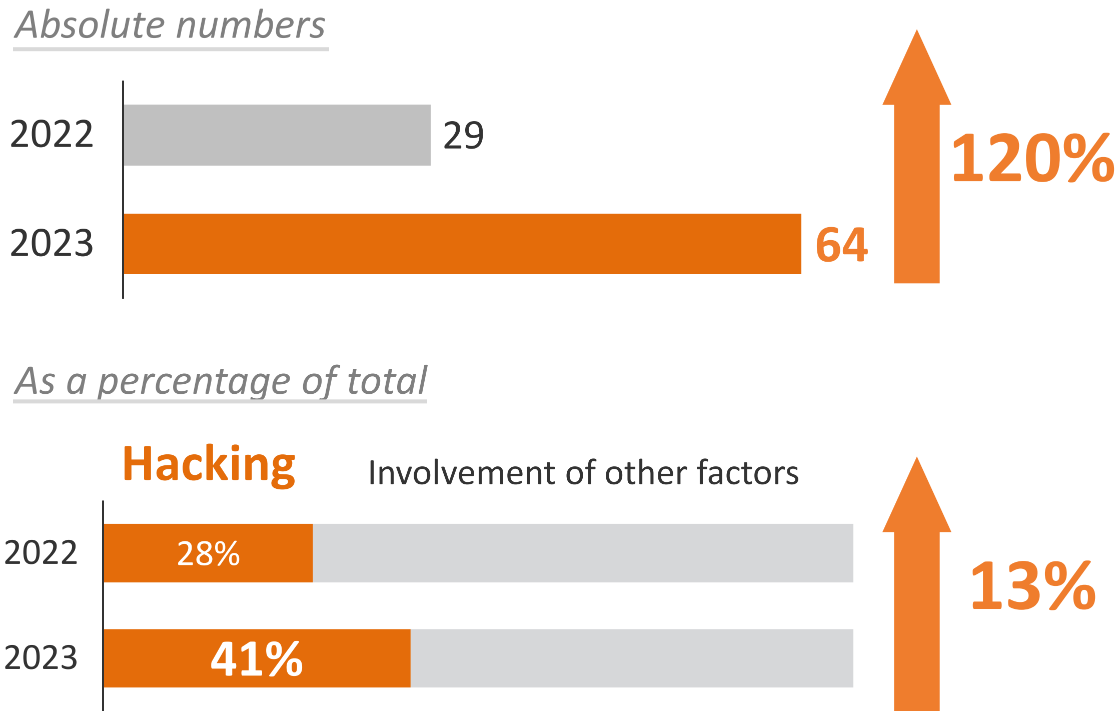
Data breach notifications to PCPD



Source: PCPD

DBNs involving hacking rose both absolutely and relatively

Data breach notifications involving hacking



Data Breach Response Plan

Putting a plan in place can help minimise impact of a data breach

PCPD
HK
PCPD.org.hk

Guidance Note

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

Guidance on Data Breach Handling and Data Breach Notifications

INTRODUCTION

Good data breach handling makes good business sense

A good data breach handling policy and practice is not only useful for containing the damage caused by a breach, but also demonstrate the data user's responsibility and accountability when tackling the problem, by formulating a clear action plan that can be followed in the event of a data breach. In addition to enabling the data subjects affected by the breach to take appropriate protective measures, data breach notifications can help reduce the risk of litigation and maintain the data user's goodwill and business relationships, and in some cases the public's confidence in the organisation.

This guidance is aimed at assisting data users to prepare for and handle data breaches, to prevent recurrence and to mitigate the loss and damage caused to the data subjects involved, particularly when sensitive personal data is involved.

What is personal data?

Data breach incidents often involve the personal data of individuals, such as customers, service users, employees and job applicants of organisations. Under the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) (PDPO), personal data means any data[1]

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable.

What is a data breach?

A data breach is generally regarded as a suspected or actual breach of the security of personal data held by a data user[2], which exposes the personal data of data subject(s) to the risk of unauthorised or accidental access, processing, erasure, loss or use.

The following are some examples of data breaches:

- ➢ The loss of personal data stored on devices such as laptop computers, USB flash drives, portable hard disks or backup tapes
- ➢
- ➢
- ➢
- ➢

[1] Section 2(1) of the PDPO.

[2] Under section 2(1) of the PDPO, a "data user", in relation to personal data, me
other persons, controls the collection, holding, processing or use of the data.

Guidance on Data Breach Handling and Data Breach Notifications 1

🤷 What

A document setting out **how** an organisation should **respond in a data breach**

The plan should outline:

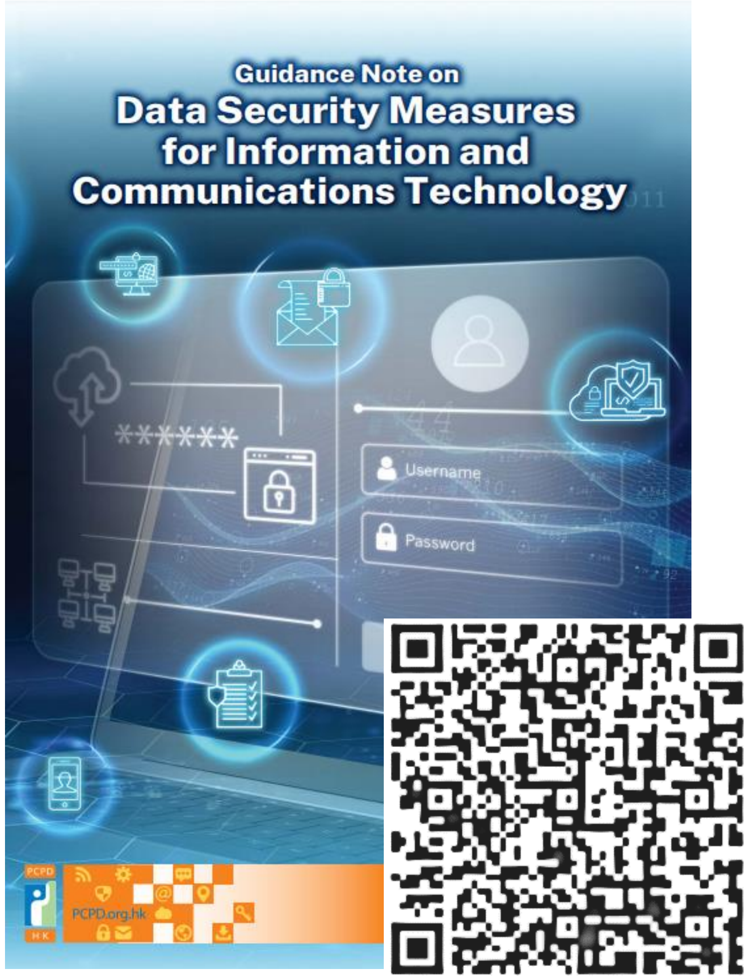
- a **set of procedures** to be followed in a data breach
- **strategy for identifying, containing, assessing and managing** the impact brought about by the incident from start to finish

❓ Why

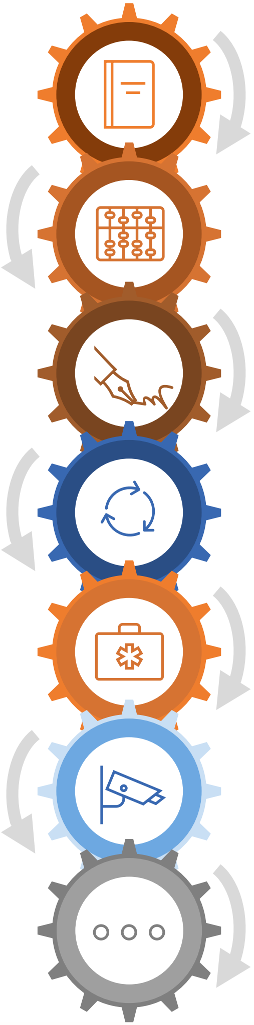
Help ensure a **quick response** to and **effective management** of a data breach

Guidance Note on Data Security Measures for ICT

We recommend best practices in strengthening data security



Guidance Note on
Data Security Measures
for Information and
Communications Technology



Data Governance & Organisational Measures

Risk Assessments

Technical and Operational Security Measures

Data Processor Management

Remedial Actions in the event of Data Security Accidents

Monitoring, Evaluation and Improvement

Other Considerations

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

數據安全熱線
Data Security Hotline
2110 1155

數據安全快測
Data Security Scanner

https://www.pcpd.org.hk/Toolkit/tc/

數據安全新!

數據安全

七大資料保安建議措施

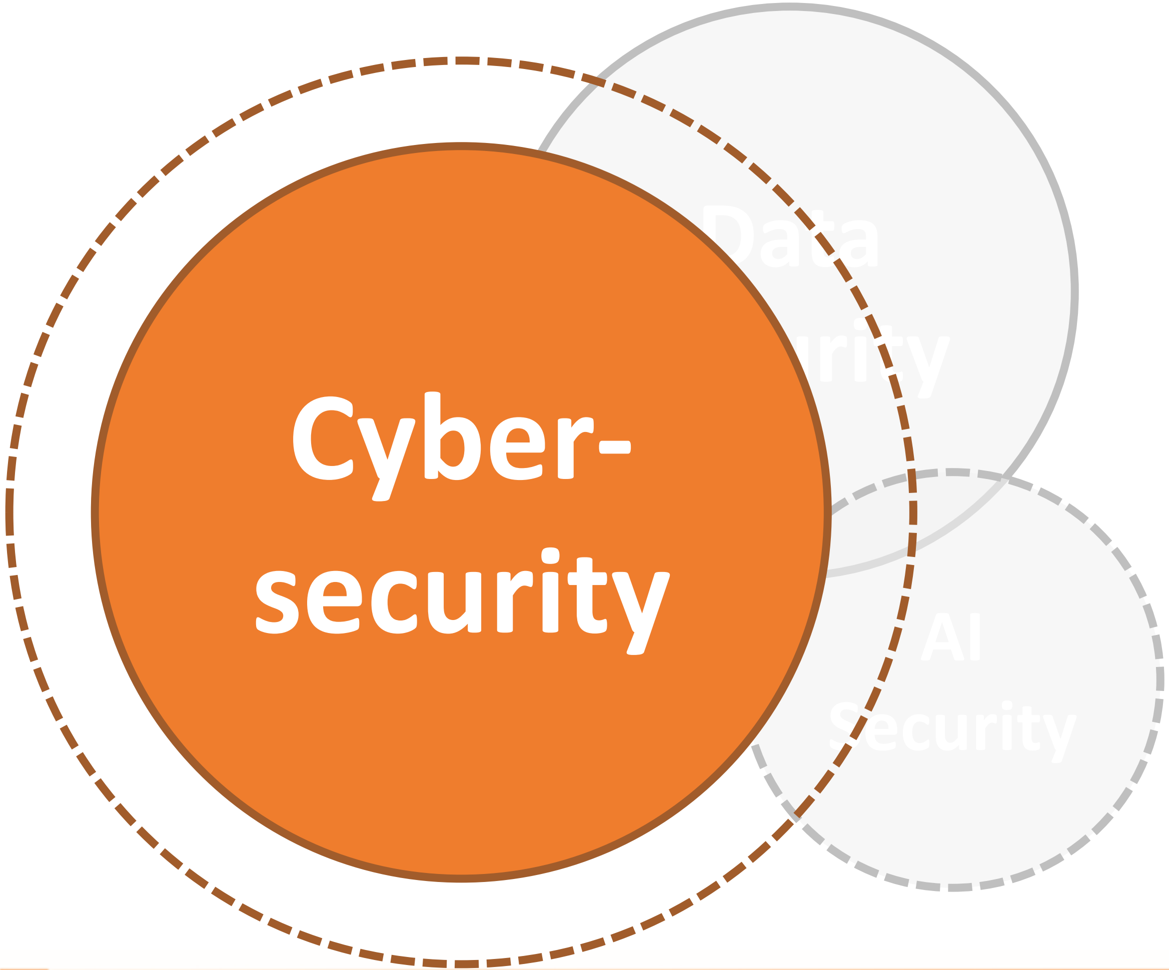
- 資料管治和機構性措施
- 風險評估
- 技術上及操作上的保安措施
- 資料處理者的管理
- 資料保安事故發生後的補救措施

數據安全專題網頁
Data Security Webpage

https://www.pcpd.org.hk/tc_chi/data_security/index.html

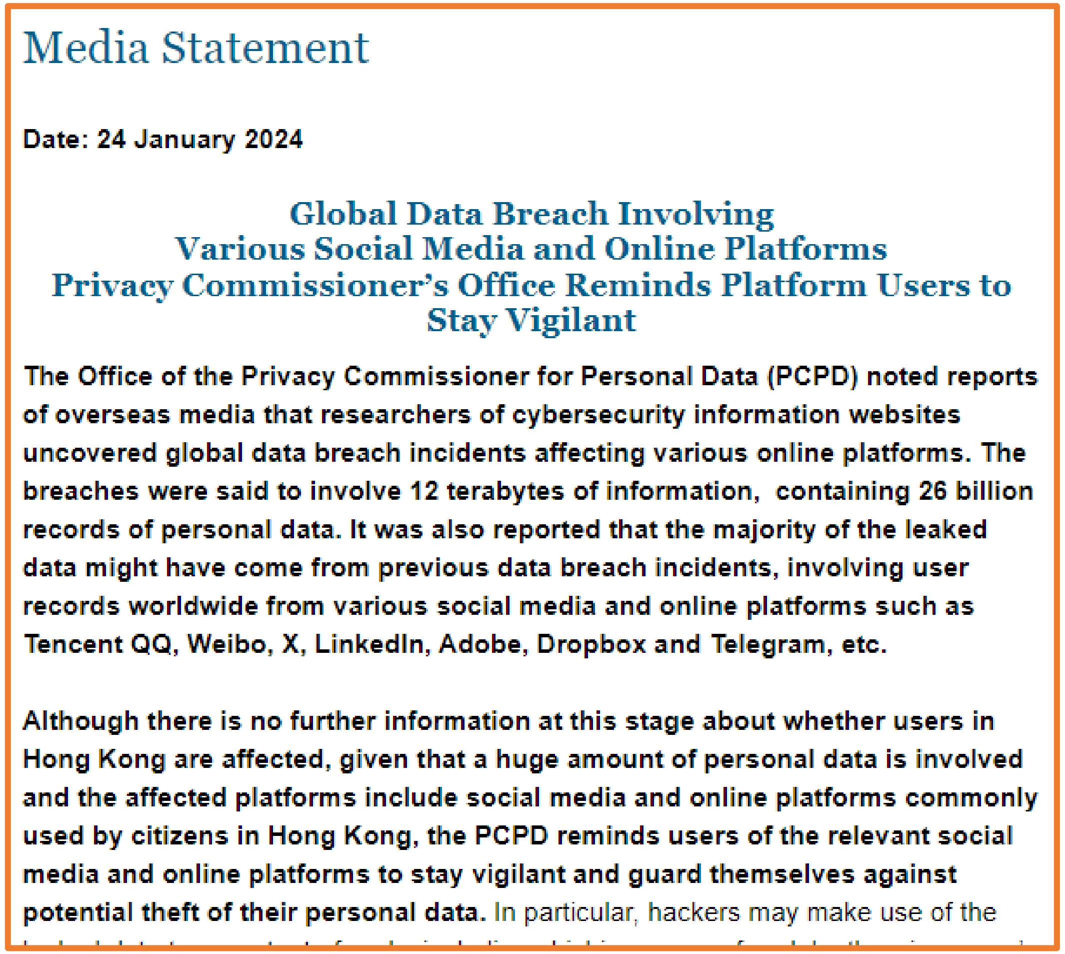
Content

We now turn to…



Global Data Breach

In Jan 2024, PCPD issued a statement reminding public to stay vigilant



Media Statement

Date: 24 January 2024

Global Data Breach Involving Various Social Media and Online Platforms Privacy Commissioner's Office Reminds Platform Users to Stay Vigilant

The Office of the Privacy Commissioner for Personal Data (PCPD) noted reports of overseas media that researchers of cybersecurity information websites uncovered global data breach incidents affecting various online platforms. The breaches were said to involve 12 terabytes of information, containing 26 billion records of personal data. It was also reported that the majority of the leaked data might have come from previous data breach incidents, involving user records worldwide from various social media and online platforms such as Tencent QQ, Weibo, X, LinkedIn, Adobe, Dropbox and Telegram, etc.

Although there is no further information at this stage about whether users in Hong Kong are affected, given that a huge amount of personal data is involved and the affected platforms include social media and online platforms commonly used by citizens in Hong Kong, the PCPD reminds users of the relevant social media and online platforms to stay vigilant and guard themselves against potential theft of their personal data. In particular, hackers may make use of the

Source: PCPD (2024)

Background

- Reports that researchers uncovered global data breach incidents affecting various online platforms involving **26 billion records of personal data**

HK data subjects

- **Affected platforms included social media and online platforms commonly used by citizens of Hong Kong**

Recommended measures

- Consider **changing password**
- Activate **multi-factor authentication**
- Beware of **unusual logins**
- Contact **credit card company** (if needed)
- Stay vigilant when you receive **suspicious calls, phishing emails**

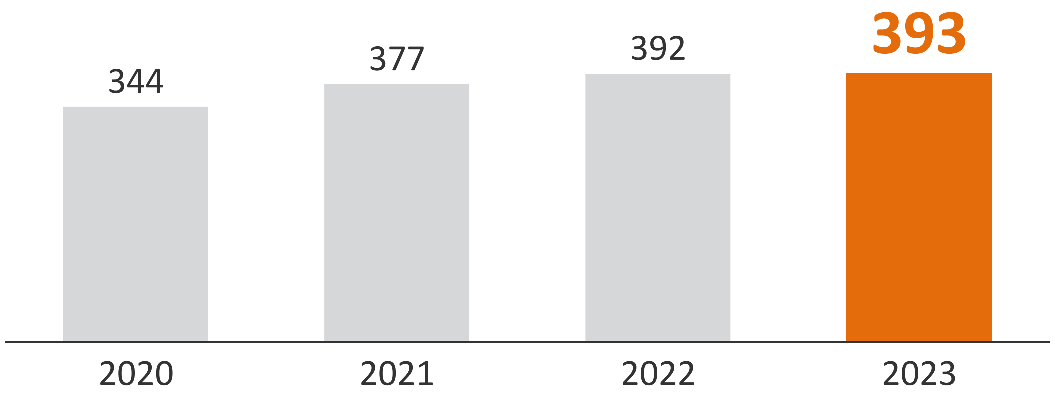
Inspections and Compliance Checks

PCPD takes proactive actions

Inspections by PCPD in the past 3 years

Report Date	Companies Inspected
9 Oct 23	ZA Bank Limited
20 Sep 23	The Registration and Electoral Office
20 Dec 22	TransUnion Limited
18 Aug 21	(1) CLP Power Hong Kong Limited and (2) The Hongkong Electric Company, Limited

✅ Compliance checks initiated by PCPD

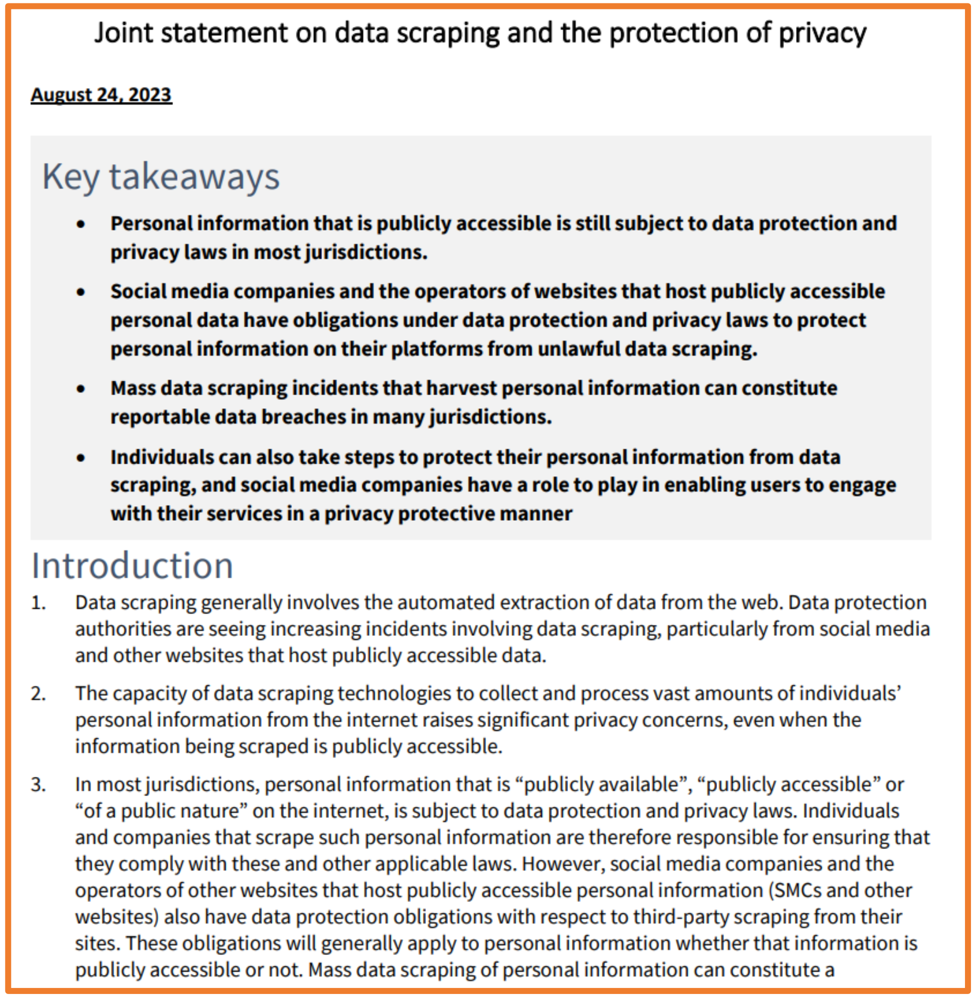


Selected compliance checks launched in 2023

- All credit reference agencies
- Users of AI systems

Global Joint Statement on Data Scraping

12 data protection authorities, including PCPD, joined hands in Aug 2023



Joint statement on data scraping and the protection of privacy

August 24, 2023

Key takeaways

- **Personal information that is publicly accessible is still subject to data protection and privacy laws in most jurisdictions.**
- **Social media companies and the operators of websites that host publicly accessible personal data have obligations under data protection and privacy laws to protect personal information on their platforms from unlawful data scraping.**
- **Mass data scraping incidents that harvest personal information can constitute reportable data breaches in many jurisdictions.**
- **Individuals can also take steps to protect their personal information from data scraping, and social media companies have a role to play in enabling users to engage with their services in a privacy protective manner**

Introduction

1. Data scraping generally involves the automated extraction of data from the web. Data protection authorities are seeing increasing incidents involving data scraping, particularly from social media and other websites that host publicly accessible data.
2. The capacity of data scraping technologies to collect and process vast amounts of individuals' personal information from the internet raises significant privacy concerns, even when the information being scraped is publicly accessible.
3. In most jurisdictions, personal information that is "publicly available", "publicly accessible" or "of a public nature" on the internet, is subject to data protection and privacy laws. Individuals and companies that scrape such personal information are therefore responsible for ensuring that they comply with these and other applicable laws. However, social media companies and the operators of other websites that host publicly accessible personal information (SMCs and other websites) also have data protection obligations with respect to third-party scraping from their sites. These obligations will generally apply to personal information whether that information is publicly accessible or not. Mass data scraping of personal information can constitute a

🏹 Aim

Highlight key privacy risks associated with data scraping

- Targeted **cyberattacks**
- **Identity fraud**
- **Unwanted direct marketing or spam**

Set out how social media companies should protect personal information of users

- **Designate** team/specific roles
- **Review** automated scraping programmes
- **Block** suspicious accounts
- **Continuously monitor** security risks and threats

Set out steps that individuals can take

- **Read privacy policies** provided by social media companies
- Think about the **amount and kinds of information** shared

Investigation into an Online Shopping Platform

Unauthorised scraping of personal data of the platform's users

Background

Data Breach Notification

The investigation arose from **a notification lodged by the company operating the online shopping platform** (the Company)

2.6 million

Personal data of 2.6 million users **posted for sale**

324,232

No. of **Hong Kong users** affected

Details

Security Vulnerability relating to a System Migration

Cause of the data breach incident found by our investigation

The Company's Obligation as a Data User

The Company has a positive duty to safeguard the security of the personal data under its control

Investigation into an Online Shopping Platform

Findings

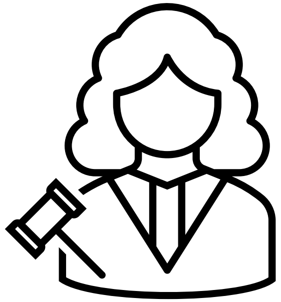
From the evidence collected in the investigation, the Privacy Commissioner considered that the incident had been caused by these deficiencies:

- Failure to check whether a **privacy impact assessment** was conducted
- Failure to check whether a **comprehensive code review process** was implemented
- Failure to ensure a **thorough security assessment** was conducted
- Failure to check and ensure that there was **a written policy** for the code review process
- Failure to ensure that **effective detection measures** were implemented

Investigation into an Online Shopping Platform

Decision

🔐 DPP4(1) contravention



The Company had **not taken all practicable steps** in relation to the system migration to ensure that the **personal data held by the Company were protected from unauthorised or accidental access, processing, erasure, loss or use,** thereby contravening DPP 4(1) concerning the **security of personal data**

The Privacy Commissioner **served an Enforcement Notice** on the Company, directing it to **remedy and prevent recurrence of the contravention**

Review of Online Platforms

We publish reports to enhance the public's awareness

Comparison of Privacy Settings of Social Media

(Apr 2022)

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
社交媒體私隱設定
大檢閱

Comparison of the Privacy Settings of 10 Online Shopping Platforms (Jun 2023)

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
數碼時代的私隱保障
比較十大網購平台的私隱設定

Online Travel Platforms

(Coming Soon)

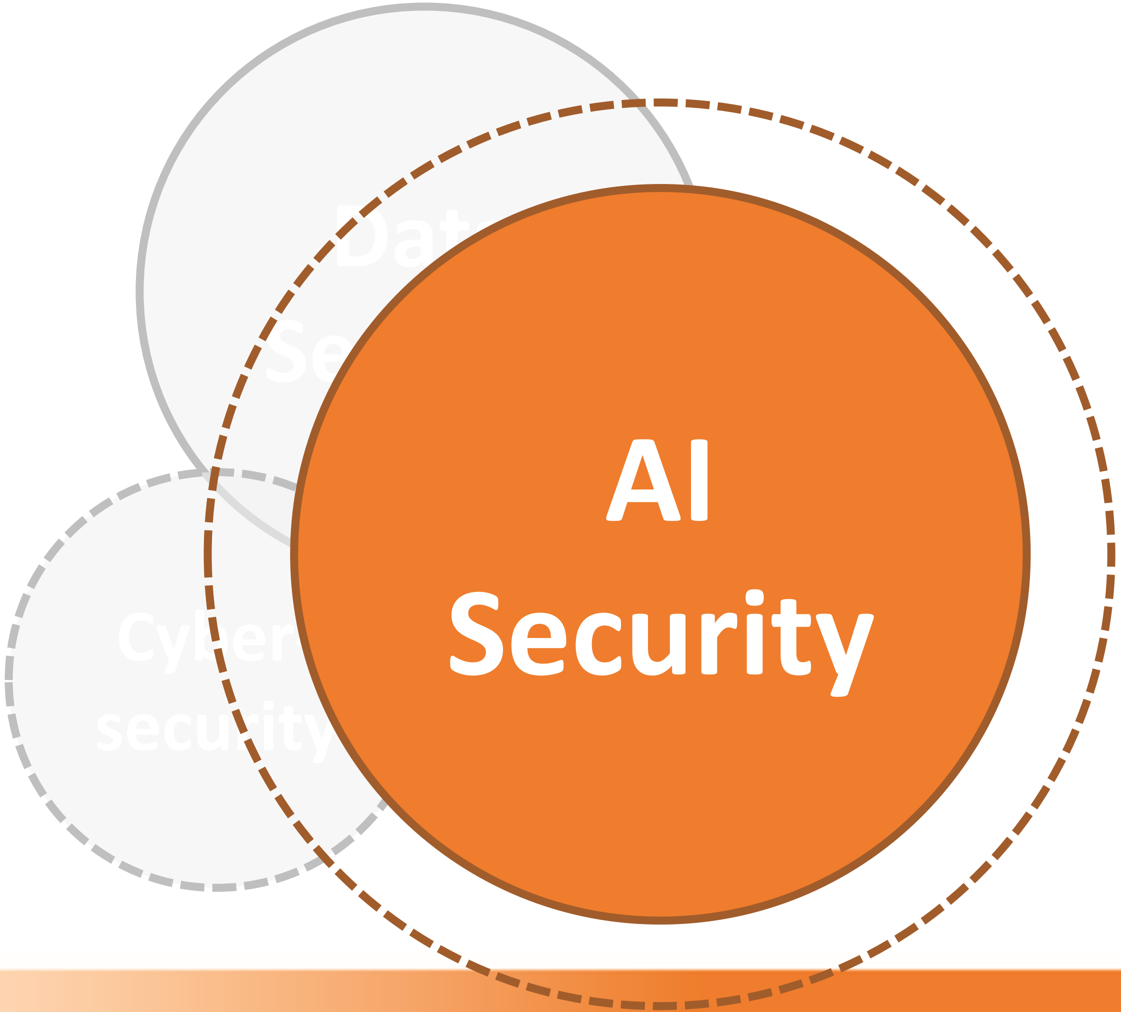
香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong
PCPD.org.hk
數碼時代的私隱保障
實測十個旅遊平台收集個人資料的情況
Hotel Booking
Travel

Tips for General Public

We issue guidelines/advisories to help enhance cybersecurity

Content

We now turn to...



Risks

AI poses privacy risks

⚡ Risk	💬 Explanation	🖼️ Illustration
Data Breach	AI systems, like chatbots, may **retain extensive user records**, making them **a target of hackers** and leading to **potential data breach**.	In March 2023, **ChatGPT** suffered a **major data breach,** revealing users' **conversation titles, names, email addresses, and the last four digits of their credit card numbers**.
Use of data	AI models can be **so advanced** that people find it **hard to understand how their personal data would be used**	Some AI models can **identify the race** of some patients even **if that is not the purpose of the models**
Excessive data collection	AI applications tend **to collect and retain as much data as possible**, including personal data	OpenAI **reportedly scraped 300 billion words online** to train ChatGPT
Data accuracy	Training AI models requires lots of data. But when **the quality and accuracy of that data are suboptimal**, the **AI system risk delivering incorrect analyses**	An AI recruitment system of a multinational company was **trained with biased data** and **favoured male over female applicants**

Deepfake

This demonstration shows how AI could easily lead to improper use of data

Global developments

Jurisdictions have taken various approaches to regulating AI

Approach

European Union

- **First comprehensive horizontal law - AI Act** (in force since Aug 2024)

Japan

- **No laws or regulations specifically to govern AI**
- **"Soft law"** (non-binding guidelines) now in place

Singapore

- **No comprehensive legislation on AI**
- **Sectoral approach**
- **PDPC published "Model AI Governance Framework" and other guidelines**

South Korea

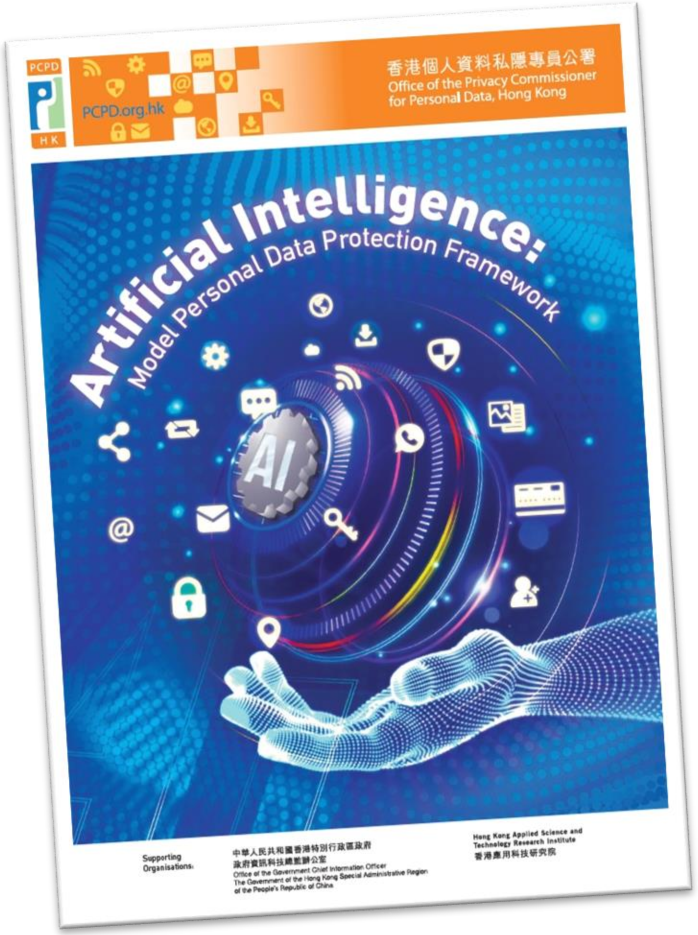
- **AI bills under consideration**
- **Existing laws** apply in the meantime
- **PIPC published "Guide to the Processing of Disclosed Personal Information for AI Development and Services"**

National developments

The Mainland has published regulatory documents covering multiple aspects of AI

	Regulatory Documents	Effective
Mainland China	- **Draft Measures for Labelling AI-Generated Synthetic Content** - **Cybersecurity technology — Labelling method for content generated by artificial intelligence**	*(Consultation ongoing)*
	- **AI Safety Governance Framework**	*Sep 2024*
	- **Basic Security Requirements for Generative Artificial Intelligence Service**	*Feb 2024*
	- Global AI Governance Initiative	*Oct 2023*
	- **Interim Measures for the Management of Generative Artificial Intelligence Services** - Practical Guidance of Cybersecurity Standards – Labelling Methods for Content Generated by Generative Artificial Intelligence Services	*Aug 2023*
	- Provisions on the Administration of Deep Synthesis of Internet-based Information Services	*Jan 2023*
	- Rules on the Management of Algorithmic Recommendations in Internet Information Services	*Mar 2022*

Artificial Intelligence: Model Personal Data Protection Framework


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
Artificial Intelligence:
Model Personal Data Protection Framework
AI
Supporting Organisations:

✨ Feature

Support Global AI Governance Initiative of the Country

AI security is one of the major areas of **national security**

A set of recommendations on the best practices for organisations **procuring, implementing and using** any type of **AI systems, including generative AI**, that involve the use of **personal data**

✅ Benefits

Assist organisations in complying with the requirements of the Personal Data (Privacy) Ordinance

Nurture the **healthy development of AI** in Hong Kong

Facilitate Hong Kong’s development into an **innovation & technology hub**

Propel **the expansion of the digital economy** not only in **HK** but also **GBA**

International standards

The Model Framework aligns with internationally recognised values and principles

Guidance on the Ethical Development and Use of

Artificial Intelligence

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

3 Data Stewardship Values

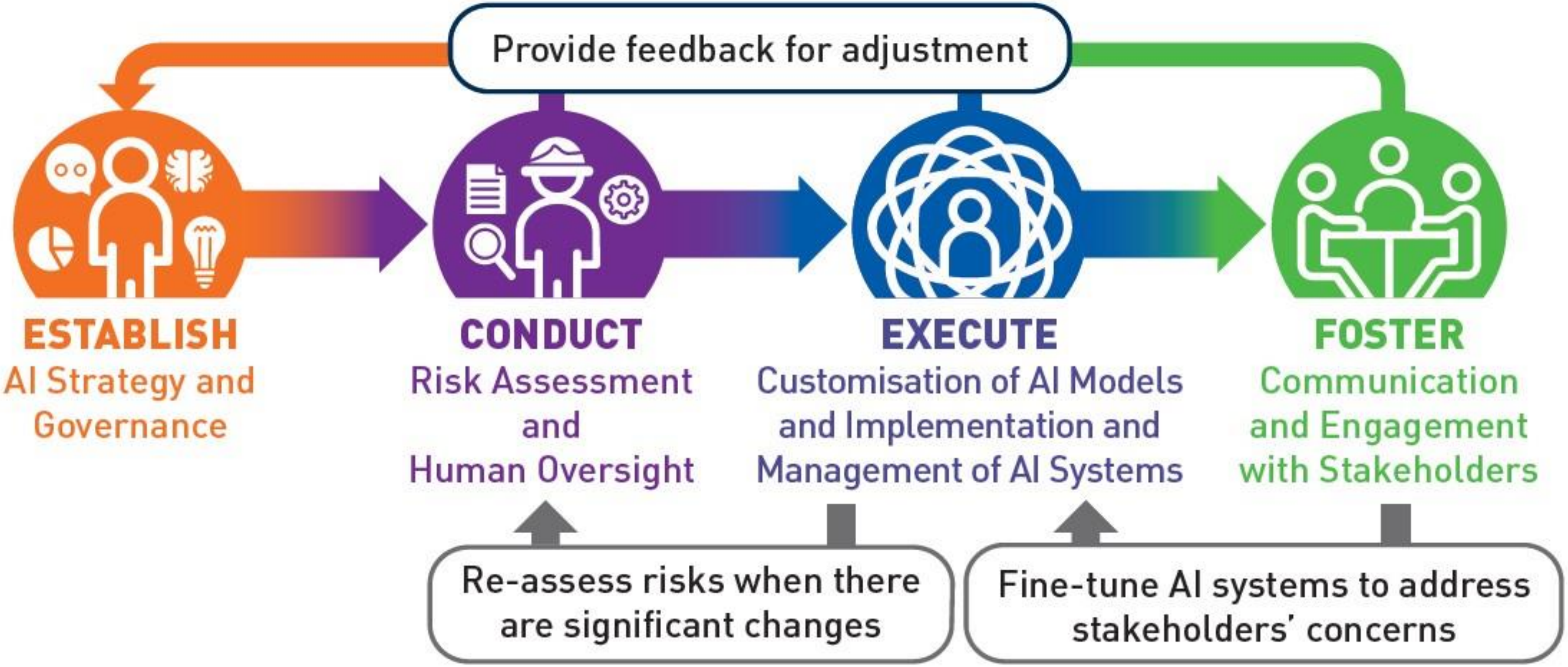
1. Being respectful
2. Being beneficial
3. Being fair

7 Ethical Principles for AI

1. Accountability
2. Human oversight
3. Transparency & interpretability
4. Data Privacy
5. Fairness
6. Beneficial AI
7. Reliability, robustness & security

Model Personal Data Protection Framework

Model Personal Data Protection Framework



Provide feedback for adjustment

ESTABLISH
AI Strategy and Governance

CONDUCT
Risk Assessment and Human Oversight

EXECUTE
Customisation of AI Models and Implementation and Management of AI Systems

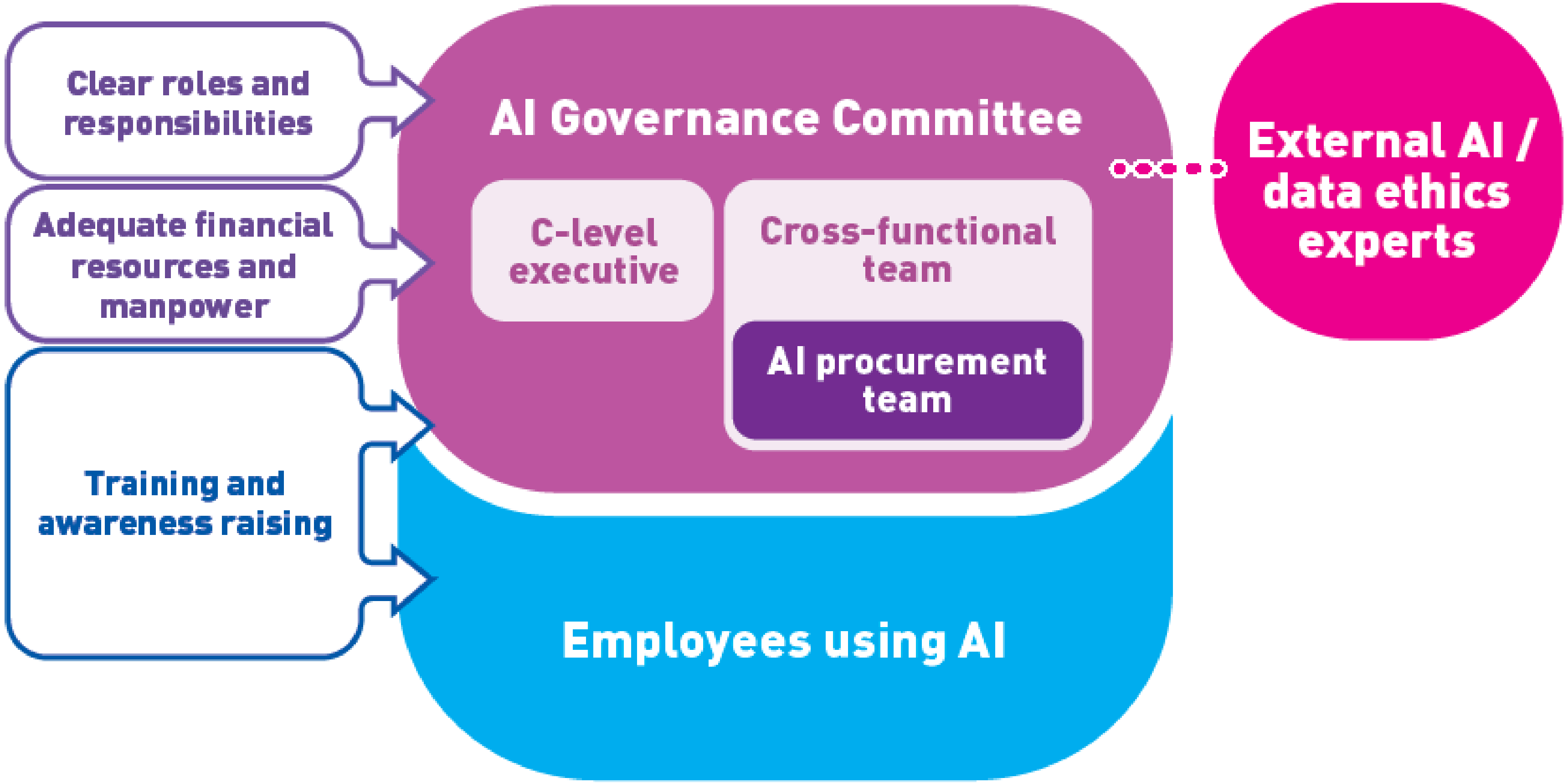
FOSTER
Communication and Engagement with Stakeholders

Re-assess risks when there are significant changes

Fine-tune AI systems to address stakeholders' concerns

Governance Structure

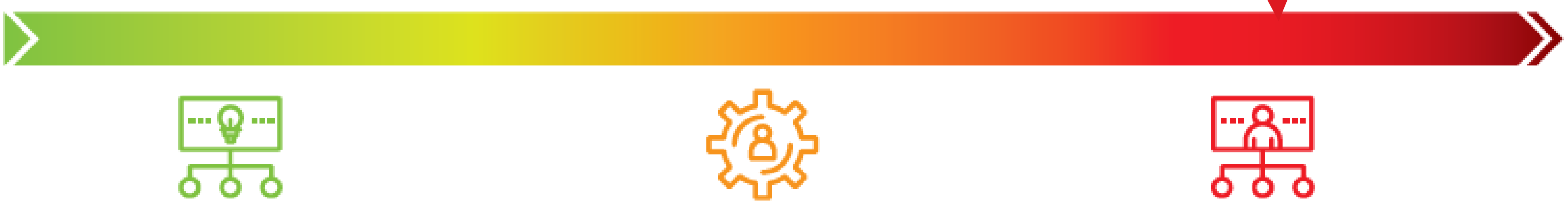
An internal governance structure with sufficient resources, expertise and authority should be established


Clear roles and responsibilities
Adequate financial resources and manpower
Training and awareness raising
AI Governance Committee
C-level executive
Cross-functional team
AI procurement team
External AI / data ethics experts
Employees using AI

Conduct Risk Assessment

The level of human oversight should correspond with the risks identified

An AI system likely to produce an output that may have such significant impacts on individuals would generally be considered high risk.



Lower **_Risk level of AI system_** *Higher*

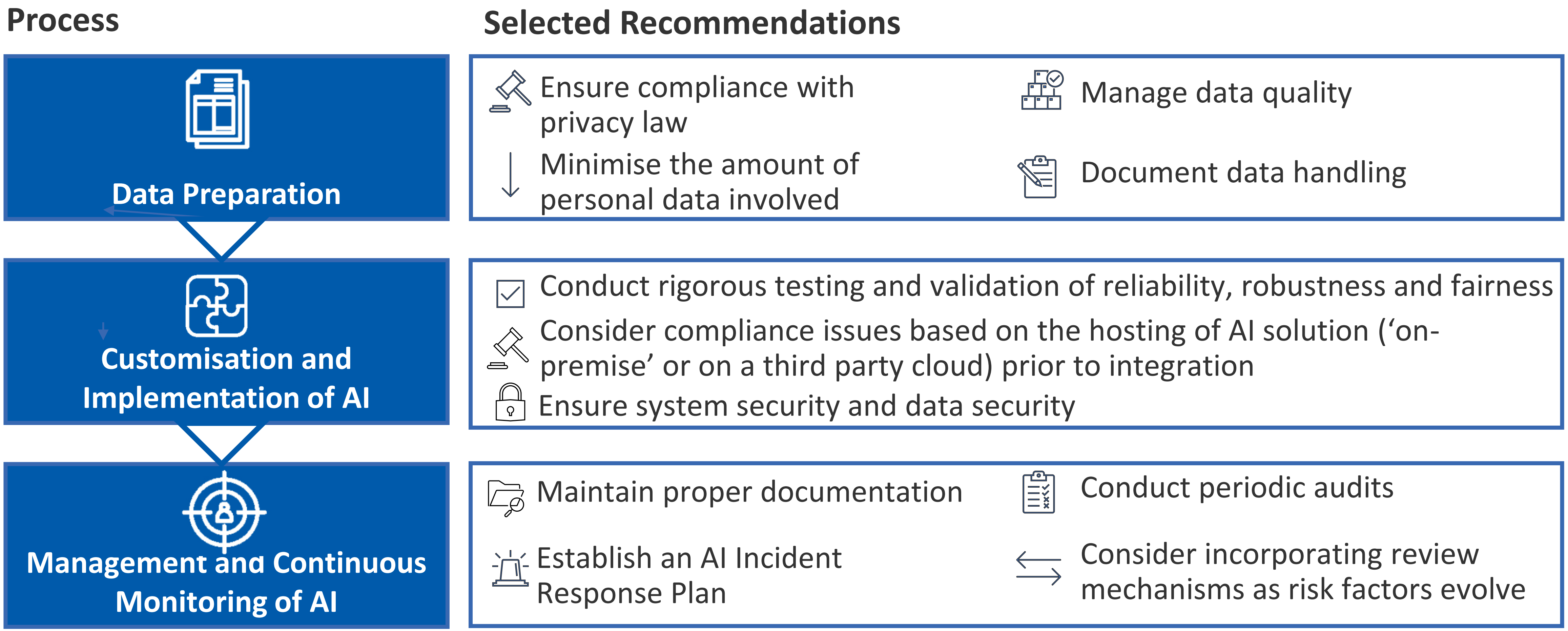
Human-out-of-the-loop
AI makes decisions without human intervention

Human-in-command
Human actors oversee the operation of AI and intervene whenever necessary

Human-in-the-loop
Human actors retain control in the decision-making process

Execute

Customisation of AI Models and implementation and management of AI systems



Process | **Selected Recommendations**

Data Preparation

- Ensure compliance with privacy law
- Minimise the amount of personal data involved
- Manage data quality
- Document data handling

Customisation and Implementation of AI

- Conduct rigorous testing and validation of reliability, robustness and fairness
- Consider compliance issues based on the hosting of AI solution (‘on-premise’ or on a third party cloud) prior to integration
- Ensure system security and data security

Management and Continuous Monitoring of AI

- Maintain proper documentation
- Establish an AI Incident Response Plan
- Conduct periodic audits
- Consider incorporating review mechanisms as risk factors evolve

AI Incident Response Plan

The plan may encompass the below six elements

1 Defining an AI Incident

2 Monitoring for AI Incidents

3 Reporting an AI Incident

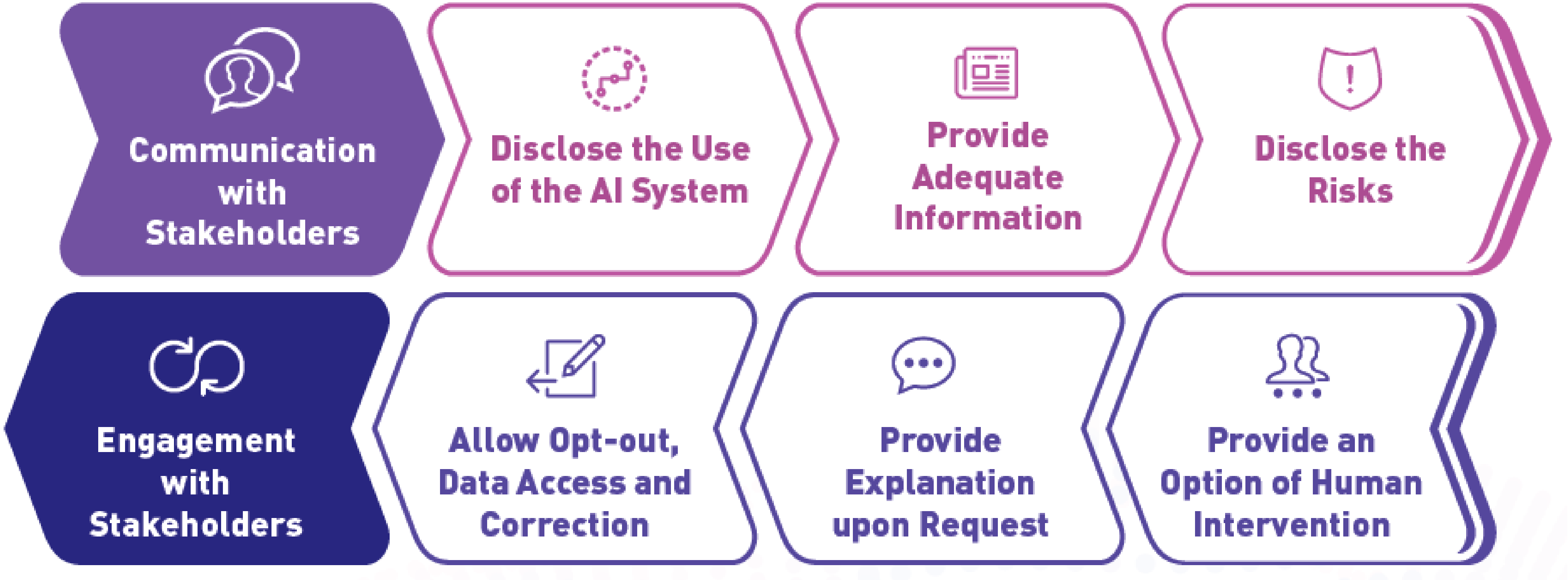
4 Containing an AI Incident

5 Investigating an AI Incident

6 Recovering from an AI Incident

Foster

Communication and engagement with stakeholders



Communication with Stakeholders

Disclose the Use of the AI System

Provide Adequate Information

Disclose the Risks

Engagement with Stakeholders

Allow Opt-out, Data Access and Correction

Provide Explanation upon Request

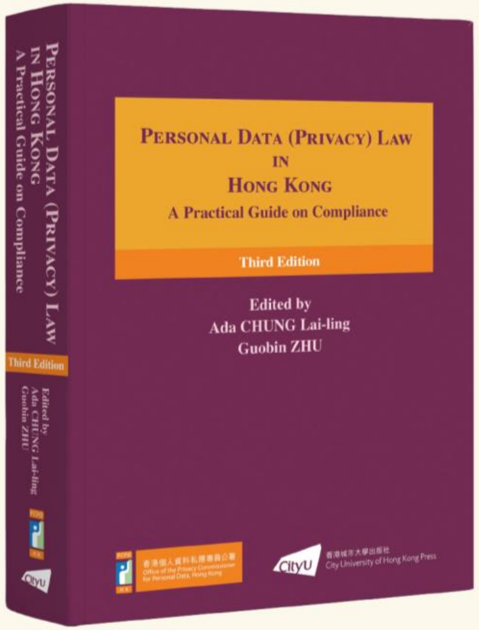
Provide an Option of Human Intervention

PERSONAL DATA (PRIVACY) LAW IN HONG KONG

A Practical Guide on Compliance (Third Edition)

Ms Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data,
Hong Kong

Professor ZHU Guobin
Professor, School of Law,
City University of Hong Kong



Highlights:

- Provisions of the PDPO on combatting doxxing
- Cross-border transfers of personal data from Hong Kong
- The Mainland's personal information protection regime
- Recent decisions by the Administrative Appeals Board and the Court
- PCPD's investigation reports and materials
- Comparison table on the personal data protection laws of Hong Kong, the Mainland and the European Union

Thank you!

www.pcpd.org.hk

communications@pcpd.org.hk

Please follow us!