



Freeman
Mathis & Gary LLP



Evolving Hong Kong Personal Data Privacy and Cybersecurity Risks and the Implications on Cyber Insurance

23 April 2025

Disclaimer

The information and opinions expressed by our speakers today are their own, and do not necessarily represent the views of their employers or of PLUS.

The contents of these materials may not be relied upon as legal advice.

Please submit questions using the question tool on the user dashboard

Meet Your Presenter

Joanne WONG

- Assistant Privacy Commissioner for Personal Data (Compliance, Global Affairs and Research)
- Office of the Privacy Commissioner for Personal Data, Hong Kong, China (PCPD)

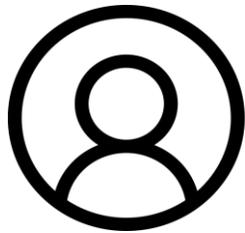


Agenda

1. Overview of the Personal Data (Privacy) Ordinance (PDPO)
2. Cyberattacks and Data Breaches
3. Artificial Intelligence (AI) and Personal Data Privacy Risks

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**



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

Who?

Three groups are involved:

Data Subject



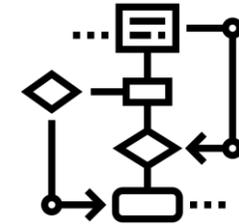
The individual who is the **subject** of the personal data

Data User



A person who, either alone or jointly or in common with other persons, **controls** the **collection, holding, processing or use** of the personal data

Data Processor



A person who –

- a) processes personal data **on behalf of another person**; and
- b) does **not** process the data for any of the person's **own purposes**

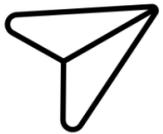
6 Data Protection Principles (DPPs)

(Schedule 1 to the PDPO)

6 保障資料原則 Data Protection Principles		
收集目的及方式 Collection Purpose & Means	1	
準確性、儲存及保留 Accuracy & Retention	2	
使用 Use	3	
保安措施 Security	4	
透明度 Openness	5	
查閱及更正 Data Access & Correction	6	

- Represent the core requirements of the **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

DPP 1 – Purpose and Manner of Collection



Personal data must be collected for a **lawful purpose directly related to a function or activity** of the data user



The data is **necessary, adequate but not excessive** in relation to the purpose of collection



The **means of collection** must be **lawful** and **fair**



All practicable steps shall be taken to **inform** the data subject whether it is obligatory to supply the personal data, the **purpose** of data collection, and the **classes of persons to whom the data may be transferred**, etc.

DPP 2 – Accuracy and Duration of Retention

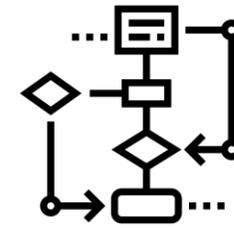
Data User



Should take **all practicable steps** to ensure:

- the **accuracy** of the personal data
- the personal data is **not kept longer than is necessary** for the fulfilment of the purpose for which the data is used

Data Processor



If a **data processor** is engaged to process personal data, the data user must adopt **contractual or other means** to prevent the personal data from being kept longer than is necessary

DPP 3 – Use of Personal Data

- Personal data shall not, without the **prescribed consent** of the data subject, be used for a **new purpose**



“New purpose” means any purpose which is unrelated to the original purpose or its directly related purpose when the data is collected

“Prescribed consent” means express consent given voluntarily which has not been withdrawn in writing

DPP 4 – Security



Data users should take **all practicable steps** to ensure the personal data that they hold is **protected against unauthorised or accidental access, processing, erasure, loss or use**



If a **data processor** is engaged, 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

DPP 5 – Openness

All Practicable Steps Should be Taken to Ensure that a Person Can:



Ascertain a data user's **policies and practices** in relation to personal data



Be informed of the **kind of personal data** held by a data user



Be informed of the main **purposes** for which personal data held by a data user is or is to be used

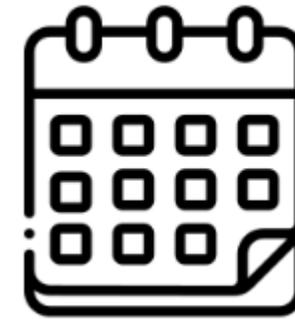
DPP 6 – Data Access and Correction



A data subject must be given **access to his personal data**



A data subject must be **entitled to request corrections** where the data is inaccurate

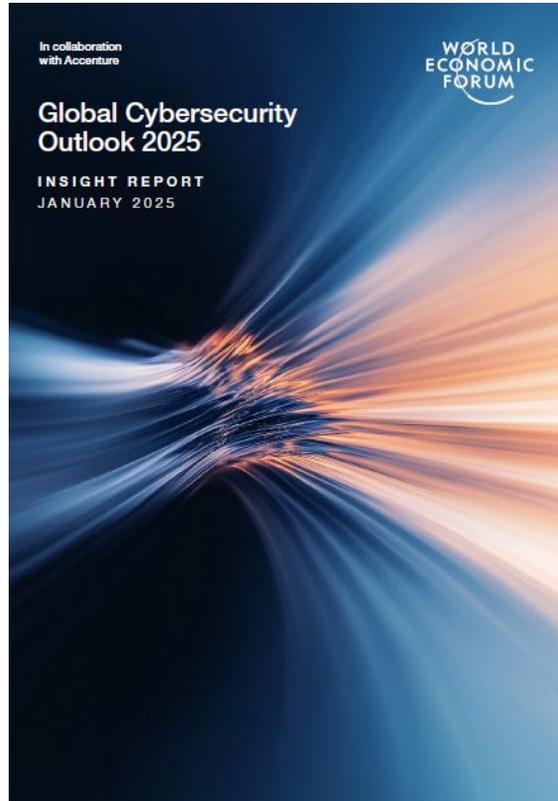


A data user must comply with a **data access or correction request within 40 days** after receipt

Agenda

1. Overview of the PDPO
2. Cyberattacks and Data Breaches
3. AI and Personal Data Privacy Risks

Global Situation

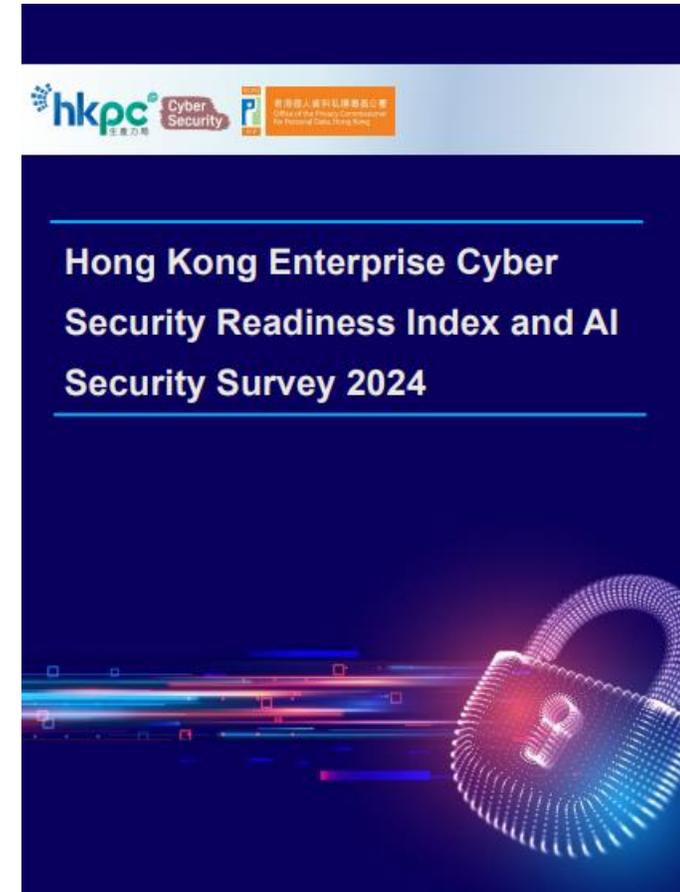
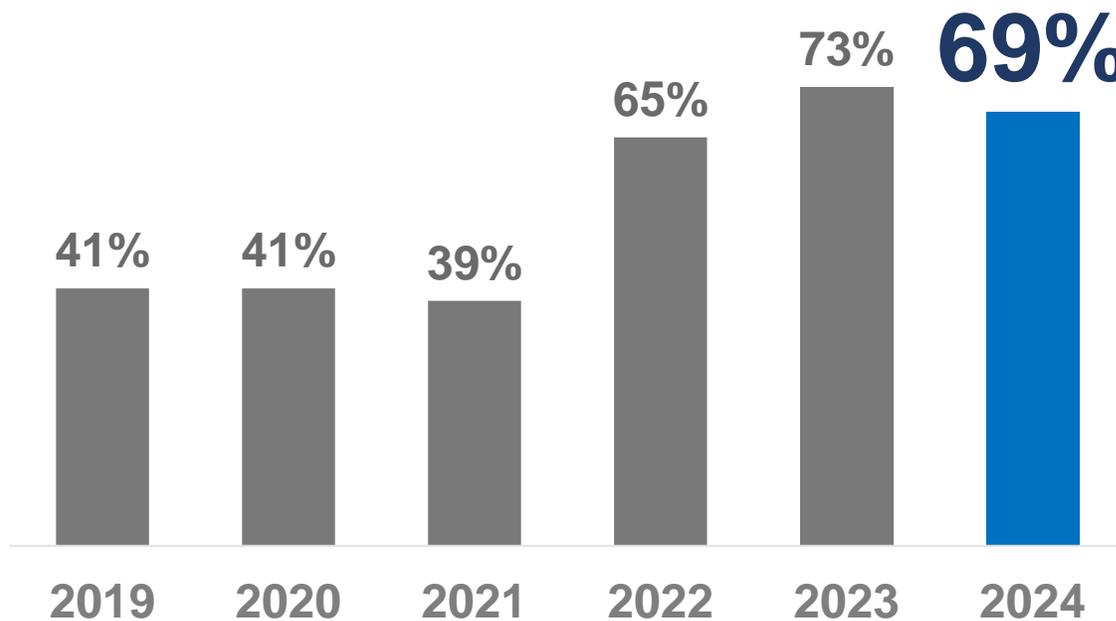


- **72%** of respondents reported an increase in organisational cyber risks, with **ransomware** remaining a top concern
- **42%** of respondents experienced **phishing** and **social engineering attacks**

Source: [WEF Global Cybersecurity Outlook 2025.pdf](#)

Local Situation – Cybersecurity Attacks

% of companies encountered cybersecurity attacks in the past 12 months



Source: [AI Security Survey 2024.pdf](#)

Local Situation – Cybersecurity Attacks

Top 5 cybersecurity attacks encountered in the past 12 months



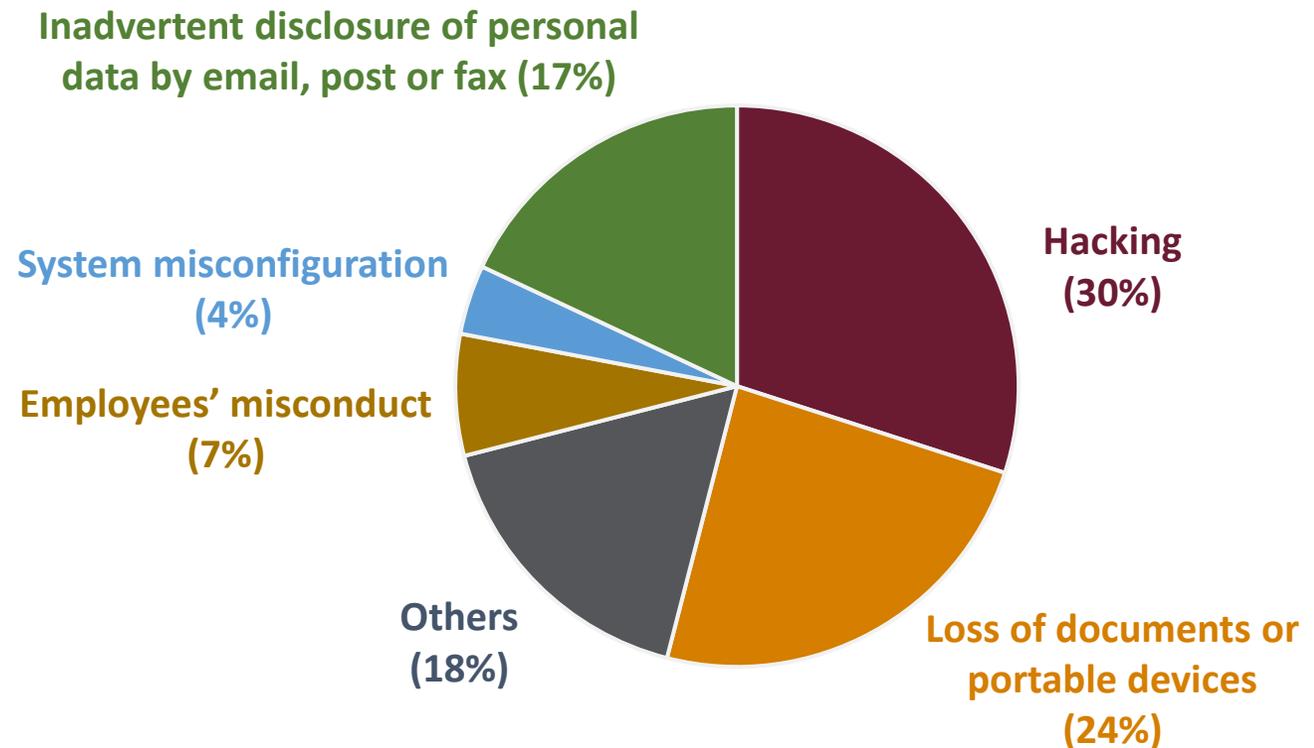
- 2** **13%** ▼2%-pt Ransomware
- 3** **11%** ▼6%-pt Other malware including Botnet
- 4** **8%** ▼6%-pt Web server & app attacks
- 5** **5%** (NA) Credential leakage or theft

▲▼ Changes compared with 2023

Source: [AISecuritySurvey2024.pdf](#)

Local Situation – Data Breaches

- In 2024, the PCPD received **203 data breach notifications (DBNs)**, which represented an increase of nearly **30%** as compared to **157** DBNs in 2023
- Among those DBNs received by the PCPD in 2024, **61** cases involved **hacking**, which constituted **30%** of all data breach incidents



Investigation

- A DBN was submitted by **a non-governmental organisation** to the PCPD, reporting that they had suffered from a **ransomware attack** which affected their information systems (Incident)
- A total of **37 servers** and **24 workstations or notebook computers** were compromised
- Over **330 GB** of data was exfiltrated from the information systems, which potentially affected around **550,000 data subjects**



Investigation Findings

Having considered the circumstances of the Incident and the information obtained during the investigation, the Privacy Commissioner found that the following **deficiencies** contributed to the occurrence of the Incident:

- 1. Outdated firewalls which contained critical vulnerabilities**
- 2. Failure to enable multi-factor authentication**
- 3. Lack of critical security patches of servers**
- 4. Ineffective detection measures in the information systems**
- 5. Inadequacies of the security assessments of information systems**
- 6. Lack of specificity of its information security policy**
- 7. Prolonged retention of personal data**

Contravention of DPPs

DPP 4(1)

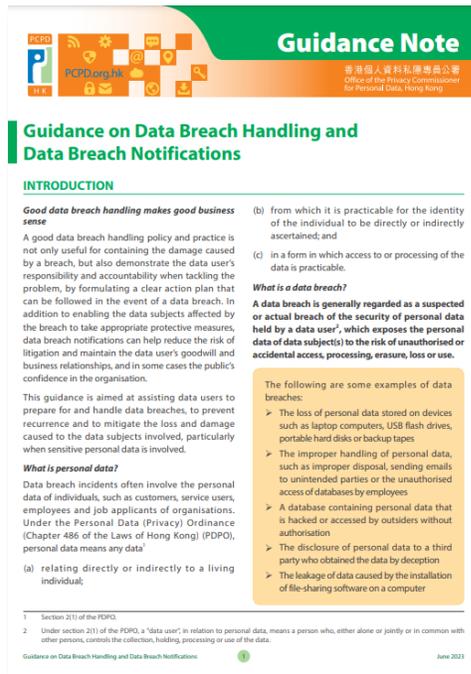
It had not taken all practicable steps to ensure that the personal data involved was **protected against unauthorised or accidental access, processing, erasure, loss or use**

DPP 2(2)

It had not taken all practicable steps to ensure that personal data was **not kept longer than was necessary for the fulfilment of the purpose** for which the data was used

“Guidance on Data Breach Handling and Data Breach Notifications”

Data Breach Response Plan



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

The plan should outline:

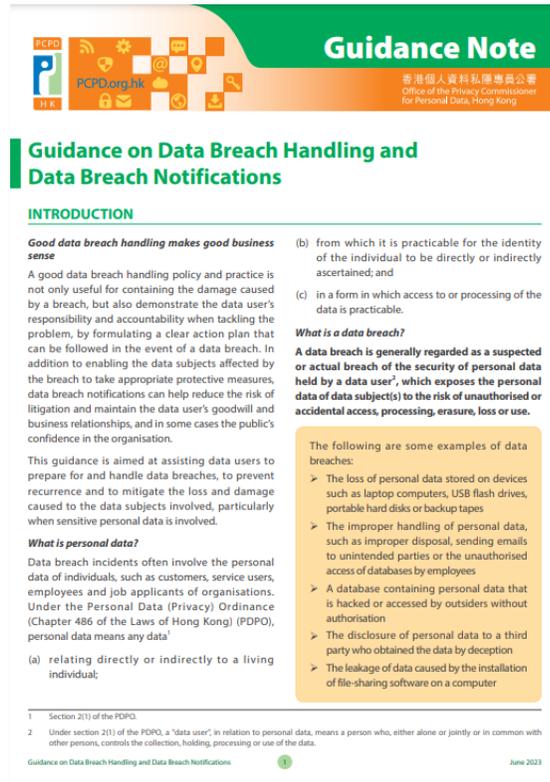
- a **set of procedures** to be followed in a data breach
- **strategy for identifying, containing, assessing and managing** the impact brought about by the incident from start to finish

Elements

- Description of what makes a data breach
- Internal incident notification procedure
- Contact details of response team members
- Risk assessment workflow
- Containment strategy
- Communication plan
- Investigation procedure
- Record keeping policy
- Post-incident review mechanism
- Training or drill plan

“Guidance on Data Breach Handling and Data Breach Notifications”

Handling Data Breaches



PCPD's Support

“Data Security” Package



Data Security Scanner



Data Security Webpage



Free Quotas to Join Professional Workshops and Seminars



Data Security Hotline

Data Security Training Series for SMEs

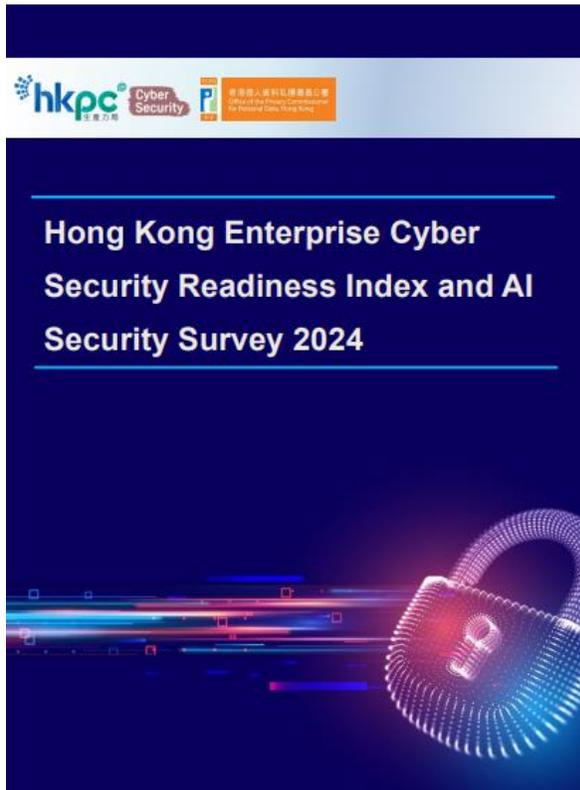
Training Jointly Rolled out by the PCPD and the HKPC. Topics include:

- Strategies to prevent cyberattacks for SMEs
- Ways and means to handle a data breach incident
- How to address the data security and privacy risks associated with AI

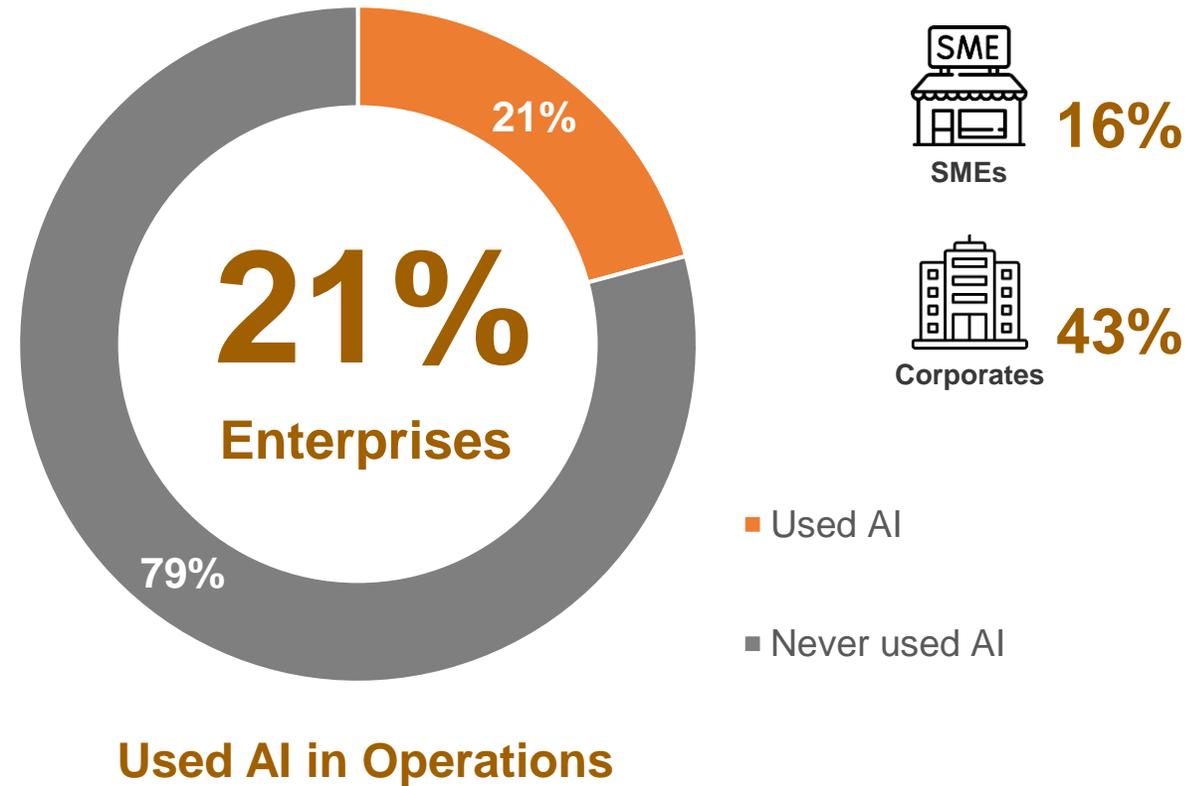
Agenda

1. Overview of the PDPO
2. Cyberattacks and Data Breaches
3. AI and Personal Data Privacy Risks

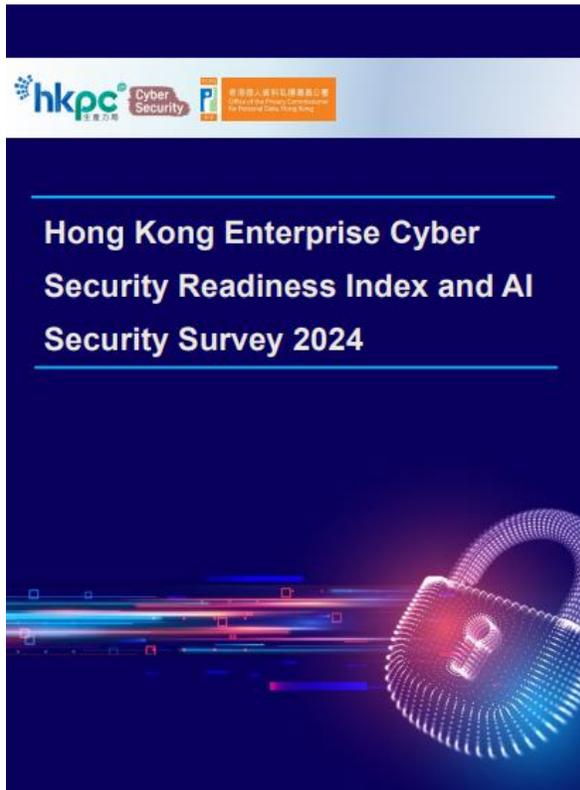
Local Situation – Enterprises’ Use of AI



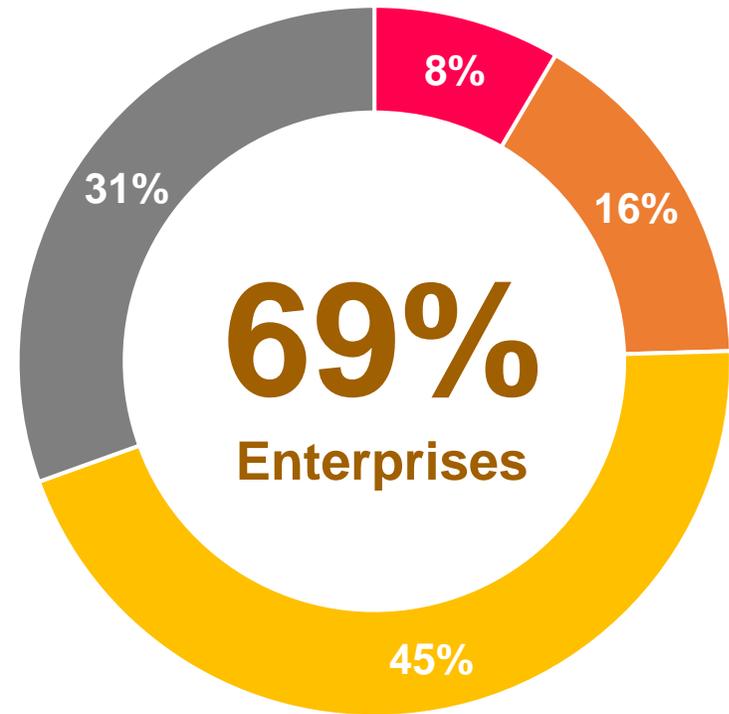
Source: [AISecuritySurvey2024.pdf](#)



Local Situation – Enterprises’ Perception on AI Risks



Source: [AISecuritySurvey2024.pdf](#)



66%



84%

- Very significant risks
- Significant risks
- Somewhat significant risks
- Insignificant risks

Perceived the Use of AI in Operations will Pose Significant Privacy Risks

Risks arising from the Use of AI

1

Privacy Risks



Excessive data collection



Misuse of data



Data security



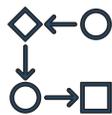
Identity re-identification



Data accuracy

2

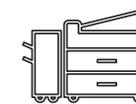
Ethical Risks



Interpretation of decisions



Harmful content



Copyright issues



Bias and inaccuracies



Hallucination

“Ethical Development and Use of Artificial Intelligence”



3 Data Stewardship Values

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



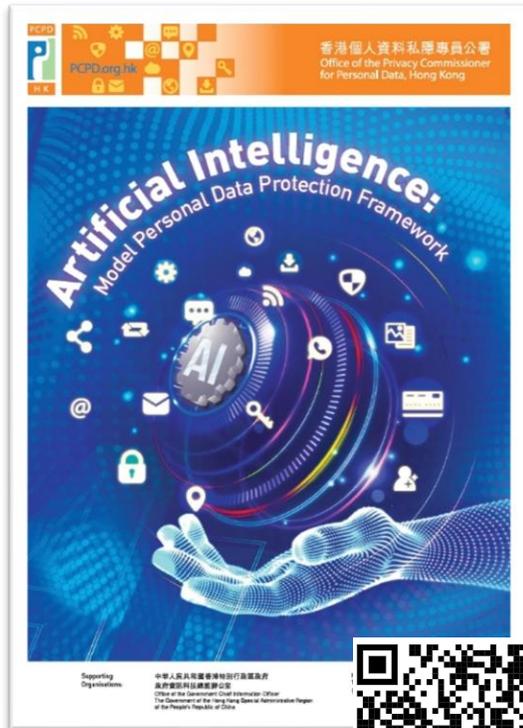
7 Ethical Principles for AI

- 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

“Artificial Intelligence: Model Personal Data Protection Framework”



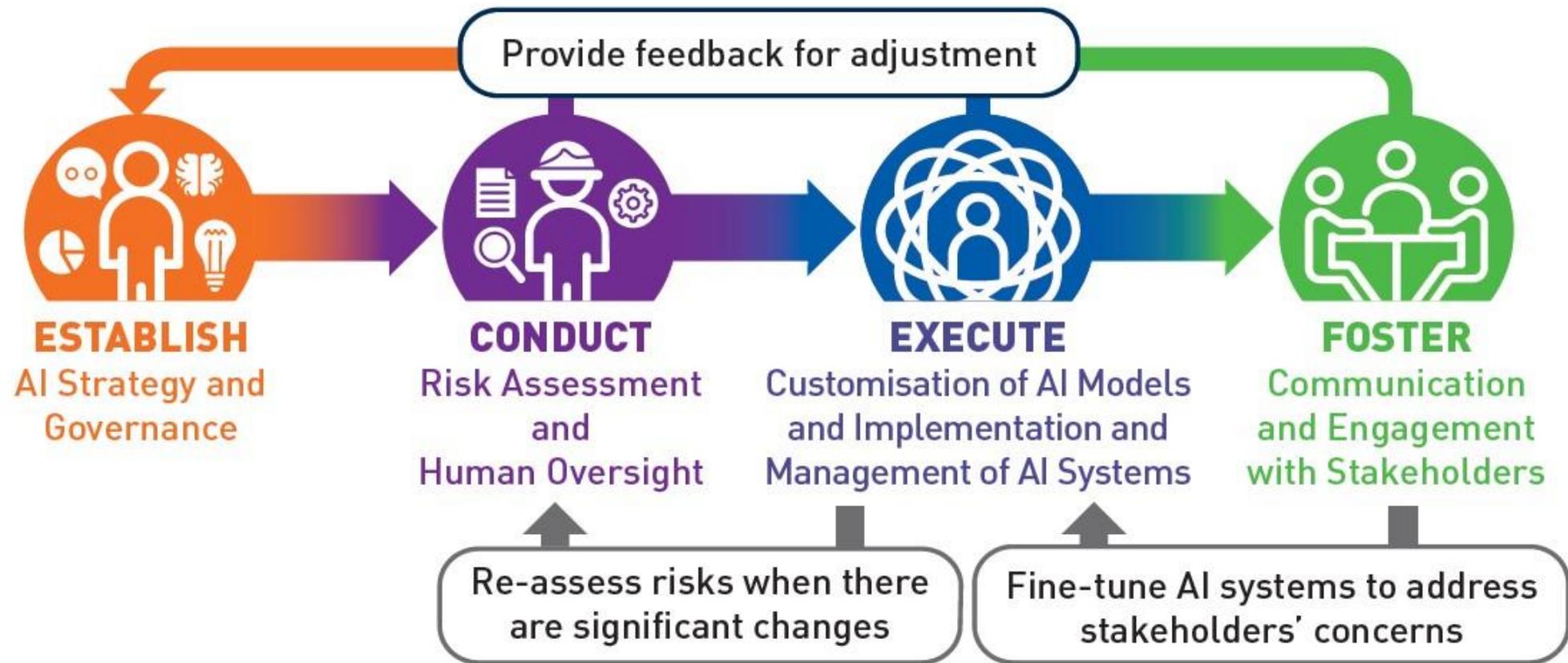
Feature

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

Benefits

-  Assist organisations in complying with the requirements of the PDPO
-  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 Hong Kong but also in the Greater Bay Area

“Artificial Intelligence: Model Personal Data Protection Framework”



AI Strategy



Functions

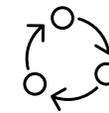
Demonstrate the commitment of top management to the ethical and responsible procurement, implementation and use of AI

Provide directions on the purposes for which AI solutions may be procured, and how AI systems should be implemented and used

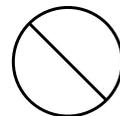
Elements that may be Included



Setting out **ethical principles**



Establishing **specific internal policies and procedures**



Determining the **unacceptable uses** of AI systems



Regularly **communicating the AI strategy**, policies and procedures



Establishing an **AI inventory**

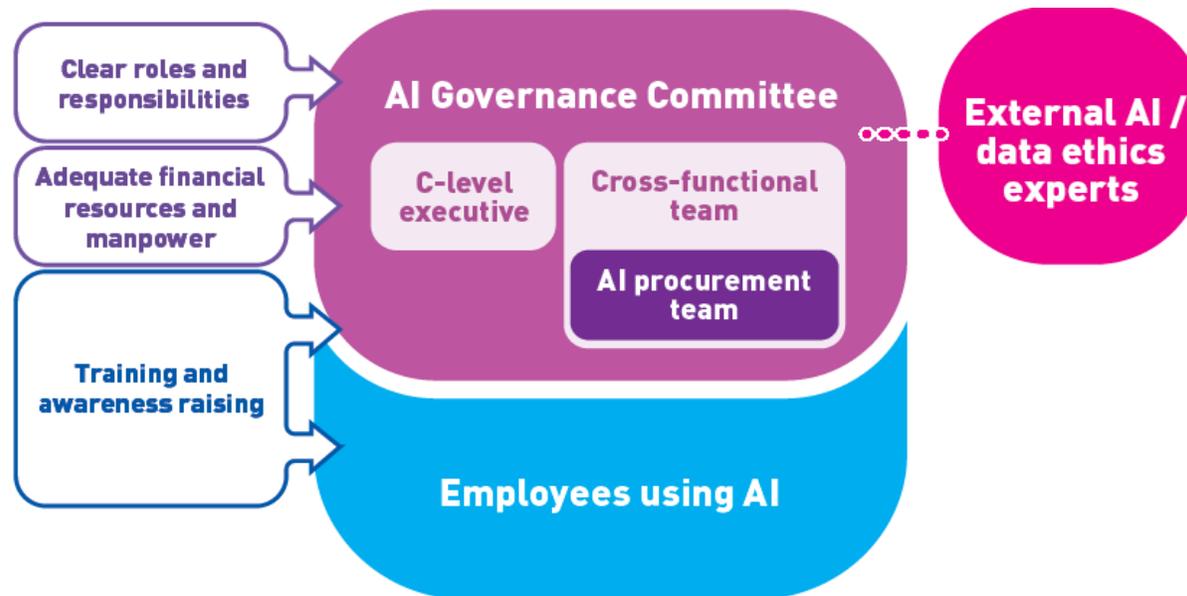


Considering **emerging laws and regulations** that may be applicable

Governance Structure



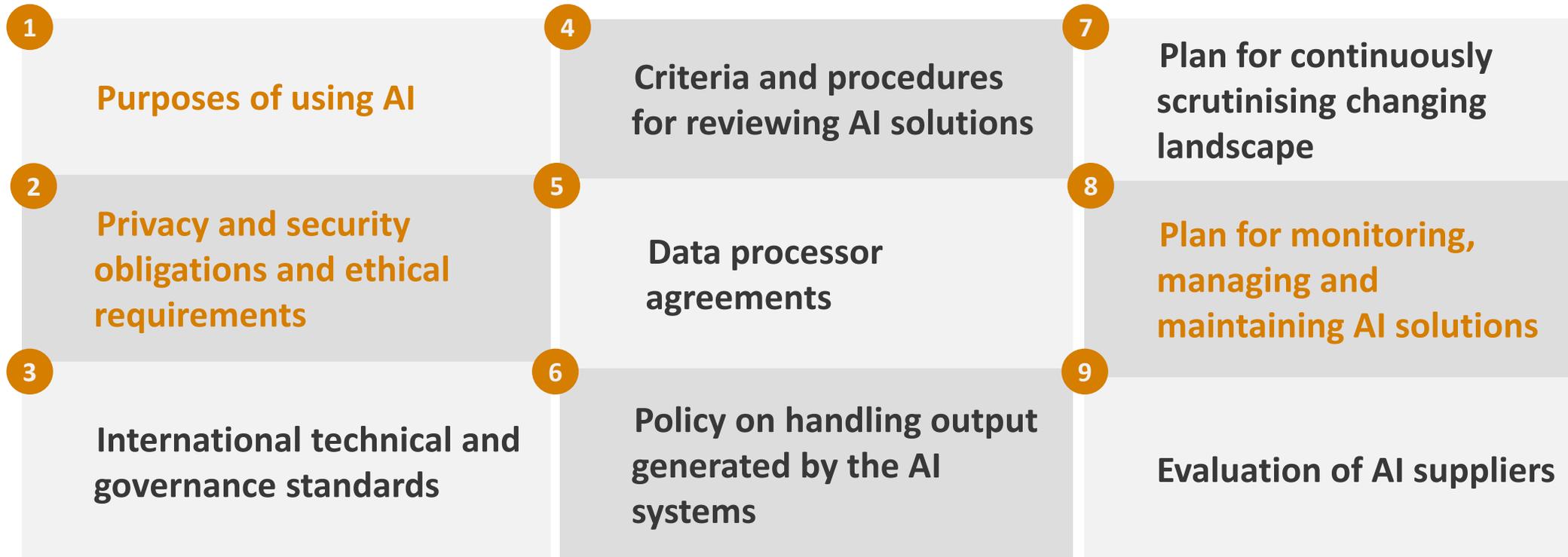
An internal governance structure with sufficient resources, expertise and authority should be established:



Governance Considerations



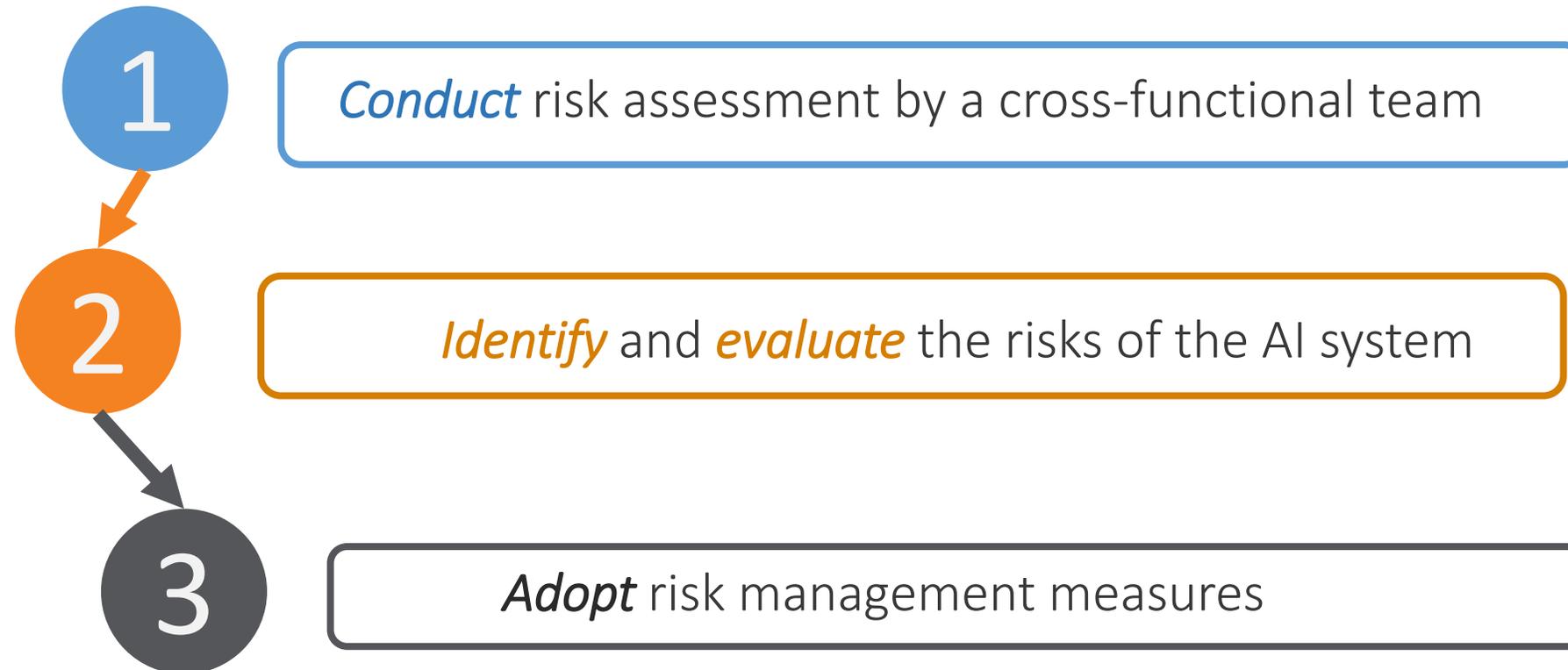
An organisation intending to invest in AI solutions may consider:



Risk Assessment and Human Oversight



Process of Risk Assessment



Risk-Based Approach

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



Customisation of AI Models and Implementation and Management of AI Systems



Process

Data Preparation



Customisation and Implementation of AI



Management and Continuous Monitoring of AI

Selected Recommendations



Ensure compliance with privacy law



Minimise the amount of personal data involved



Manage data quality



Document data handling



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



Maintain proper documentation



Establish an AI Incident Response Plan



Conduct periodic audits



Consider incorporating review mechanisms as risk factors evolve

Foster Communication and Engagement with Stakeholders



1

**Information
provision**

3

Explainable AI

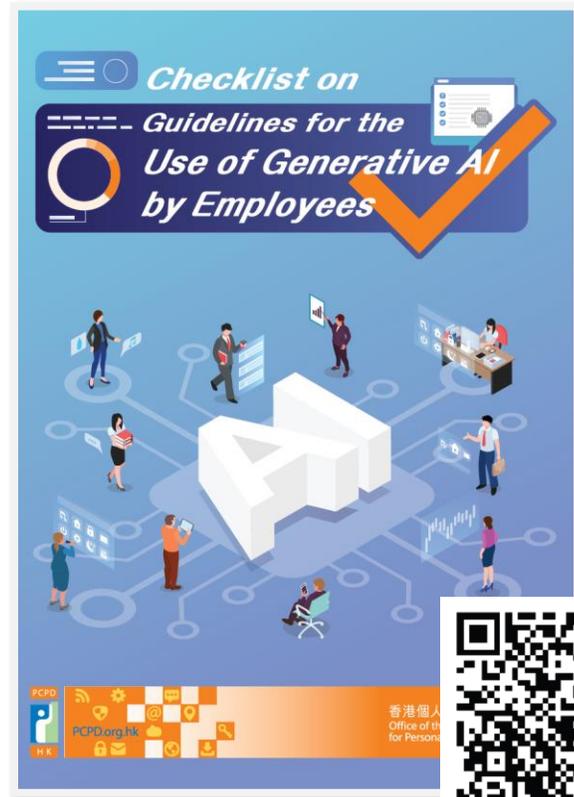
2

**Data subject rights
and feedback**

4

**Language and
manner**

“Checklist on Guidelines for the Use of Generative AI by Employees”



- Presented in a **checklist format**
- As a matter of good practice, organisations may devise their own policies or guidelines **in alignment with their values and mission**
- Helps organisations develop internal policies or guidelines for employees’ use of Gen AI at work while **complying with the requirements of the PDPO** in relation to the handling of personal data

Recommended Coverage of the Policies or Guidelines

Scope

Protection of personal data privacy

Lawful and ethical use and prevention of bias

Data security

Violations of the policies or guidelines

Thank you!

Thank you to the PLUS Diamond Sponsors

