PCPD
H K

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

AI and Personal Data Protection: Challenges and Recommendations on Governance

Cyber Security Summit Hong Kong 2024

24 October 2024

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data

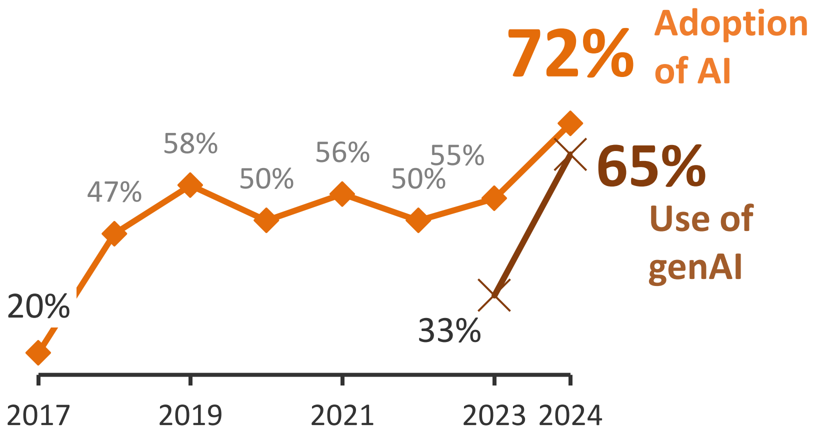
Rising trend

Organisations have used AI more and more – at a rapid rate

Global AI (including genAI) adoption rate has soared

Organisations that have adopted AI in at least 1 business function

% of respondents

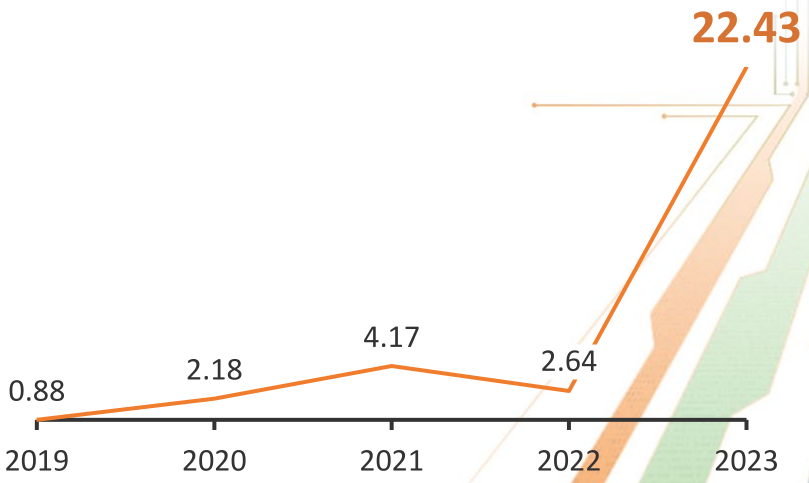


Source: McKinsey

Global investments in genAI have surged

Private investment in genAI

Total investment, US$ billions (constant 2021 US$)



Source: Our World in Data

Privacy Risks

AI poses personal data 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.**

Organisation’s awareness and readiness

Organisations see genAI as posing higher privacy risks

Perceived privacy risks levels of emerging technologies

Hong Kong enterprises, 2023

Ranked 1st

1 Generative AI

2 Cookies and other online trackers

3 Cloud computing

4 Internet of Things

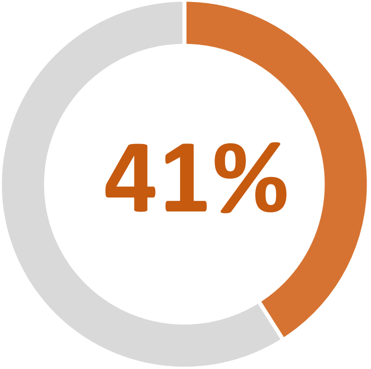
5 Blockchain related technology

6 Data analytics and work process automation

Few enterprises implemented internal guidelines for Gen AI use

Enterprises using Gen AI which implemented internal guidelines

2023



hkpc Cyber Security

Hong Kong Enterprise Cyber Security Readiness Index and Privacy Awareness Survey 2023

Source: PCPD & HKPC

Best of both worlds

Is it possible to enjoy benefits of AI while ensuring privacy protection?

Privacy risks need to be carefully managed

Benefits of AI can be enjoyed

Source: AI-generated image from Microsoft Copilot

Global developments

Jurisdictions have taken various approaches to regulating AI

Regulatory Approaches

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”**

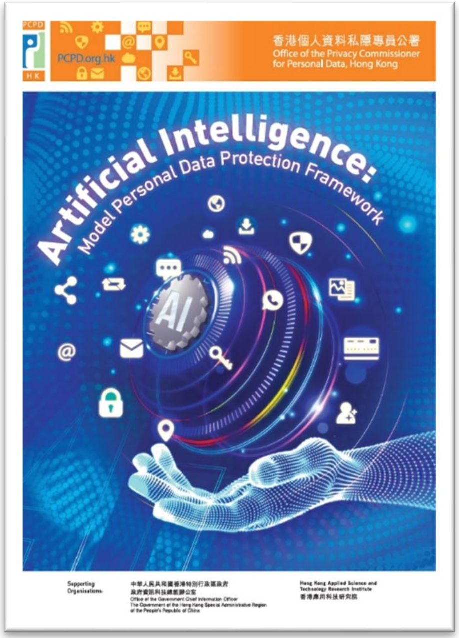
National developments

The Mainland has published regulatory documents covering multiple aspects of AI

Mainland China

Regulatory Documents	Effective
- **Draft Measures for Labelling AI-Generated Synthetic Content**	*(Consultation ongoing)*
- **Cybersecurity technology — Labelling method for content generated by artificial intelligence**	
- 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	*Aug 2023*
- Practical Guidance of Cybersecurity Standards – Labelling Methods for Content Generated by Generative Artificial Intelligence Services	
- 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



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

Artificial Intelligence:
Model Personal Data Protection Framework

Supporting Organisations

中華人民共和國香港特別行政區政府
政府資訊科技總監辦公室
Office of the Government Chief Information Officer
The Government of the Hong Kong Special Administrative Region
of the People's Republic of China

Hong Kong Applied Science and
Technology Research Institute
香港應用科技研究院

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

Foundation of the Framework

The Framework aligns with internationally recognised values and principles

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

1996-2021
守護 · 私隱 · 廿五載

3 Data Stewardship Values

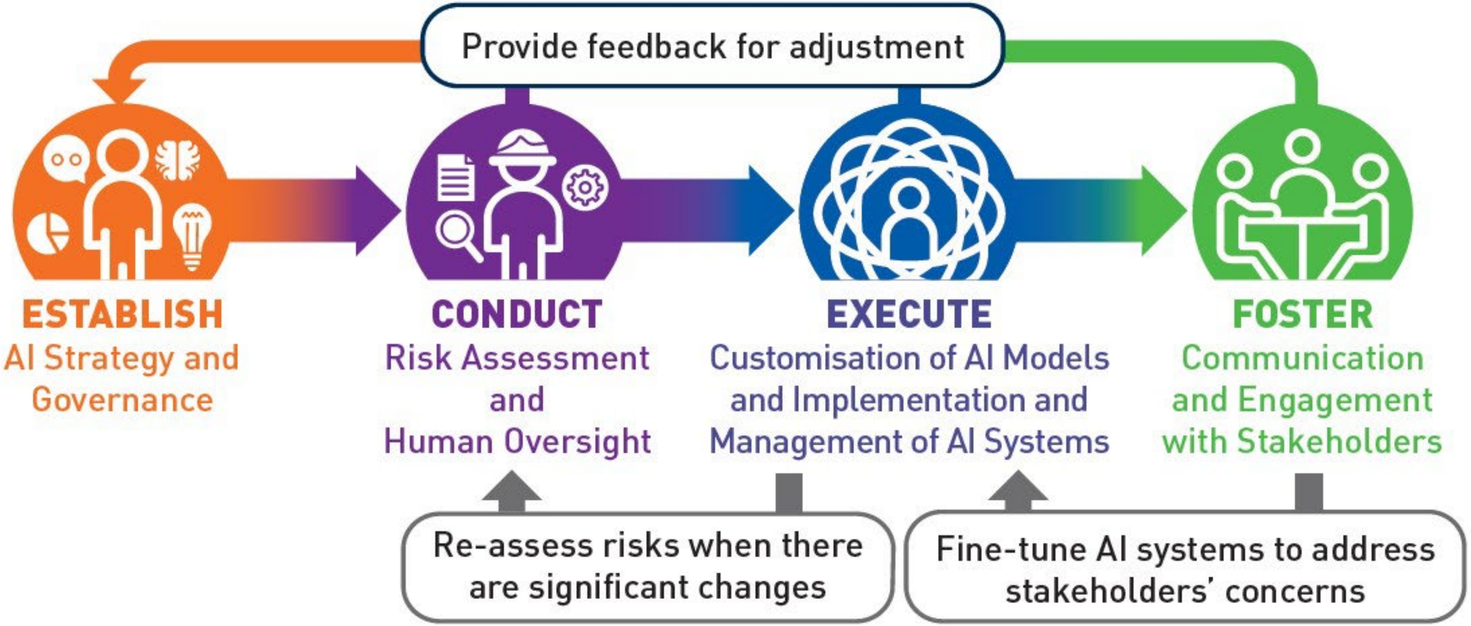
1. Being respectful
2. Being beneficial
3. Being fair

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



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 considerations

An organisation intending to invest in AI solutions may consider

ESTABLISH
AI Strategy and Governance

1.1 AI Strategy

1.2 Governance Considerations

1.3 Governance Structure

1.4 Training

- Purpose(s) of using AI
- Privacy and security obligations and ethical requirements
- International technical and governance standards
- Criteria and procedures for reviewing AI solutions
- Data processor agreements
- Policy on handling output generated by the AI system
- Plan for continuously scrutinising changing landscape
- Plan for monitoring, managing and maintaining AI solution
- Evaluation of AI supplier

Governance Structure

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

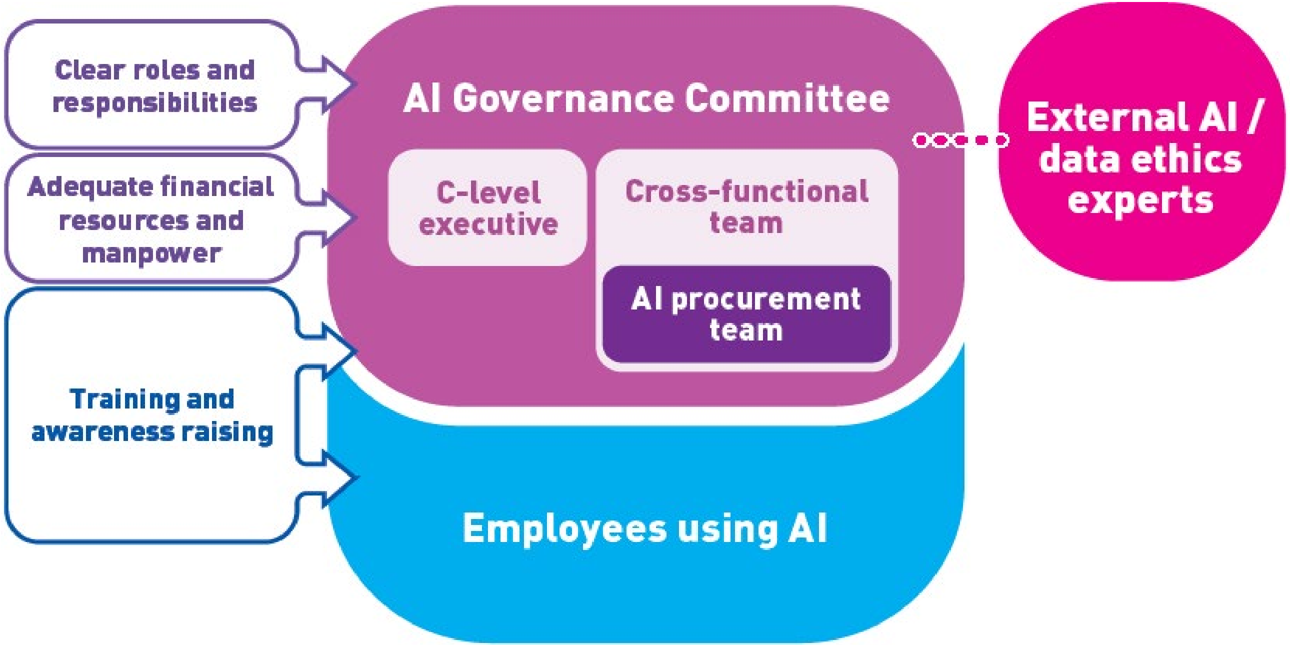
ESTABLISH
AI Strategy and Governance

1.1 AI Strategy

1.2 Governance Considerations

1.3 Governance Structure

1.4 Training

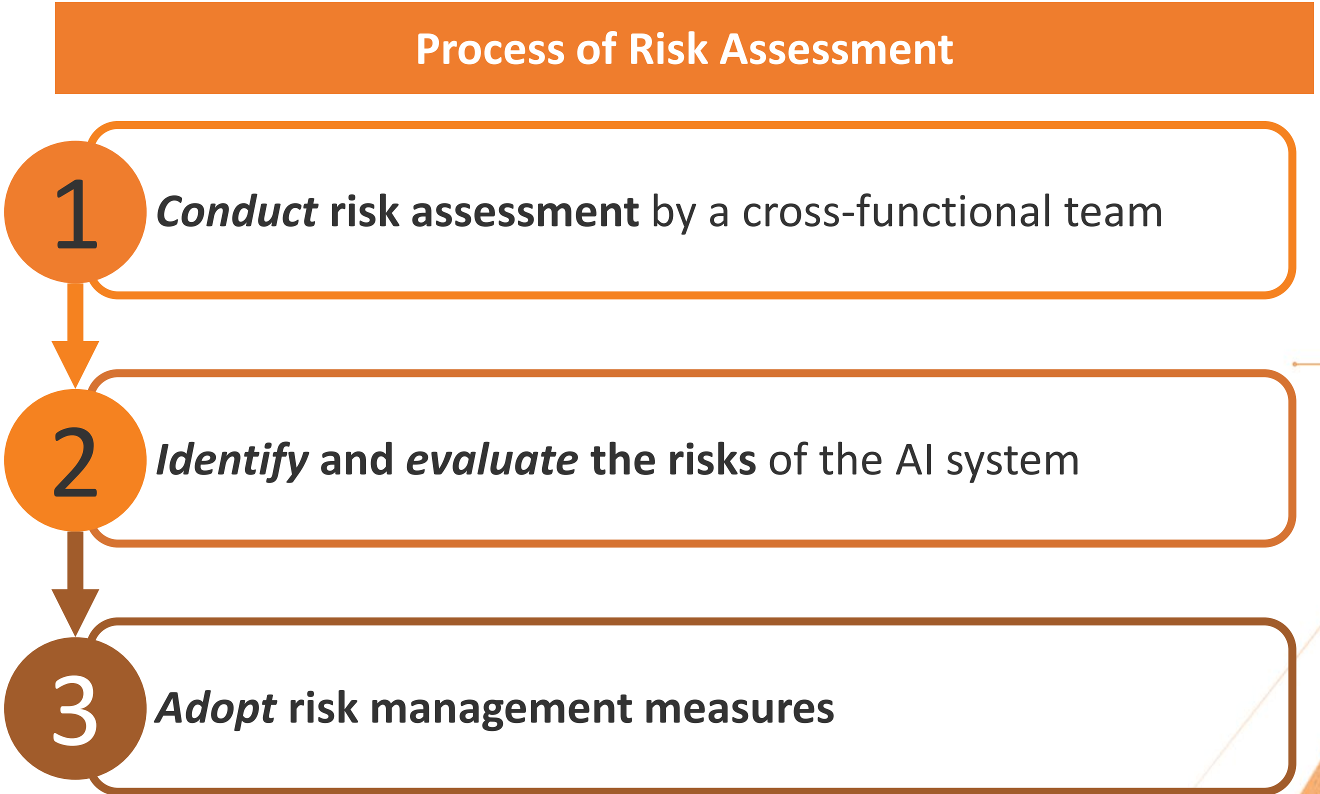


Clear roles and responsibilities
Adequate financial resources and manpower
Training and awareness raising
AI Governance Committee
C-level executive
Cross-functional team
AI procurement team
External AI / data ethics experts
Employees using AI

Conduct

Risk assessment and human oversight

CONDUCT
Risk Assessment
and
Human Oversight



Process of Risk Assessment

1. ***Conduct* risk assessment** by a cross-functional team

2. ***Identify* and *evaluate* the risks** of the AI system

3. ***Adopt* risk management measures**

Risk-based approach

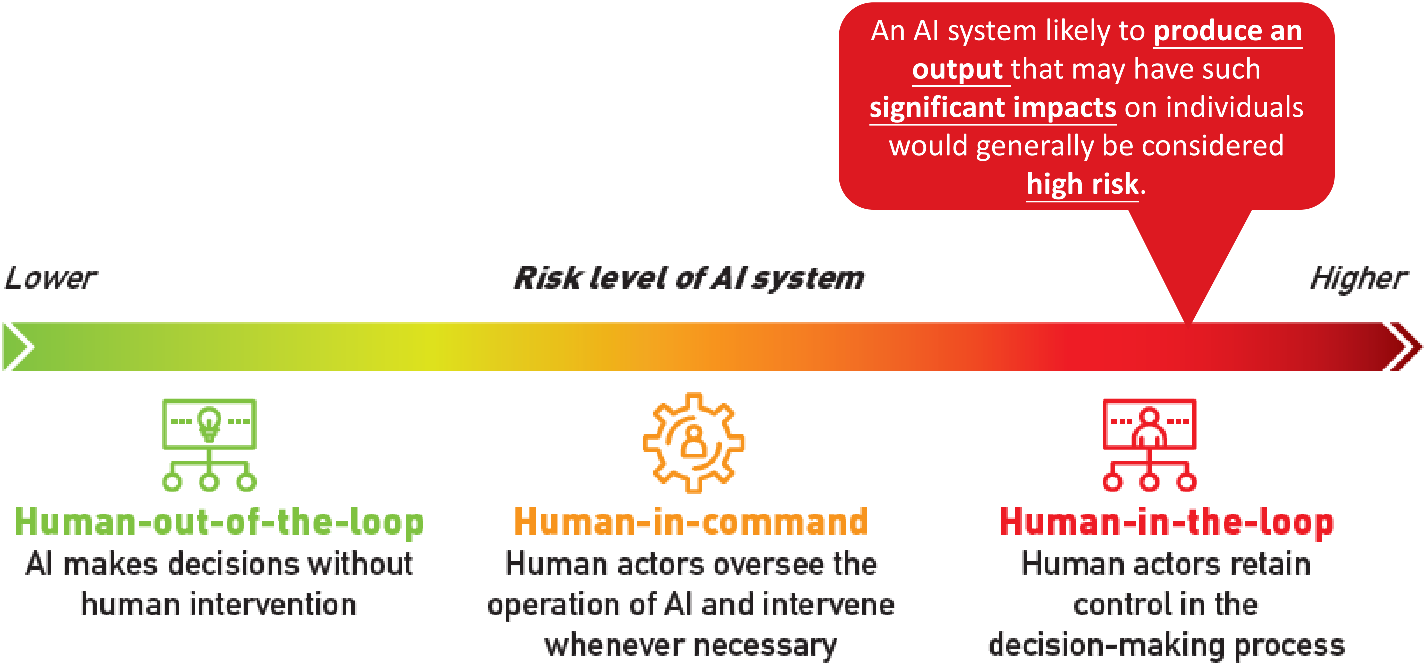
The level of human oversight should correspond with the risks identified

CONDUCT
Risk Assessment
and
Human Oversight

2.1 Risk Factors

2.2 Human Oversight

2.3 Risk Mitigation Trade-offs



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

Examples

The below use cases may incur higher risks

CONDUCT
Risk Assessment
and
Human Oversight

2.1 Risk Factors

2.2 Human Oversight

2.3 Risk Mitigation Trade-offs

- Real-time identification of individuals using biometric data
- Evaluation of individuals' eligibility for social welfare or public services
- Assessment of job applicants, evaluation of job performance or termination of employment contracts
- Evaluation of the creditworthiness of individuals for making automated financial decisions
- AI-assisted medical imaging analytics or therapies

Execute: Data Preparation

Compliance, data minimization, quality management, data handling

PCPD H K

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

3.1 Data Preparation

3.2 Customisation Implementation

3.3 Management & Monitoring

Selected Recommendations

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

Example

- A **fashion retail platform** is **purchasing a third-party developed AI chatbot** that it will customise to provide **fashion recommendations** to its customers
- The company may find it **necessary** to use the **past purchases** and **browsing histories** of **different segments** of its customer groups to fine-tune the chatbot
- However, the use of **personal data**, such as customers’ names, contact details and certain demographic characteristics, would **not be necessary**

Execute: Customisation of AI Models and implementation and management of AI systems

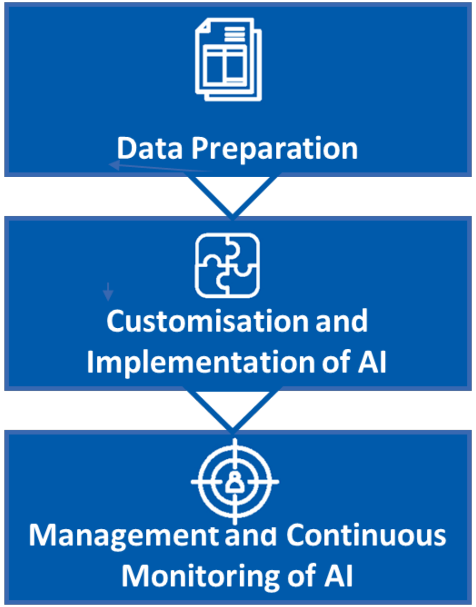
EXECUTE
Customisation of AI Models and Implementation and Management of AI Systems

3.1 Data Preparation

3.2 Customisation Implementation

3.3 Management & Monitoring

Process


Data Preparation
Customisation and Implementation of AI
Management and Continuous Monitoring of AI

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

All six steps in a glance

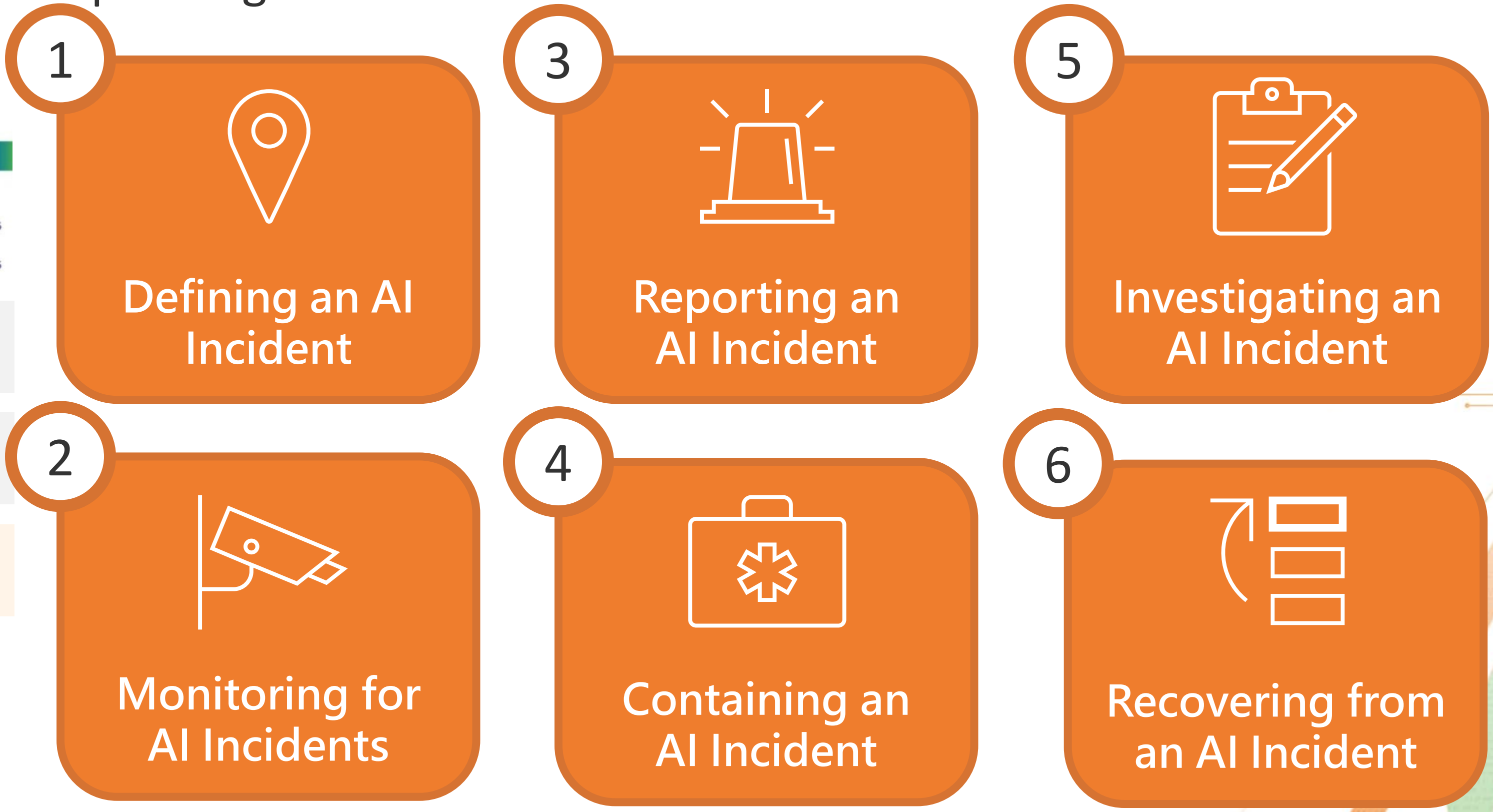
EXECUTE

Customisation of AI Models and Implementation and Management of AI Systems

3.1 Data Preparation

3.2 Customisation Implementation

3.3 Management & Monitoring



1 Defining an AI Incident

2 Monitoring for AI Incidents

3 Reporting an AI Incident

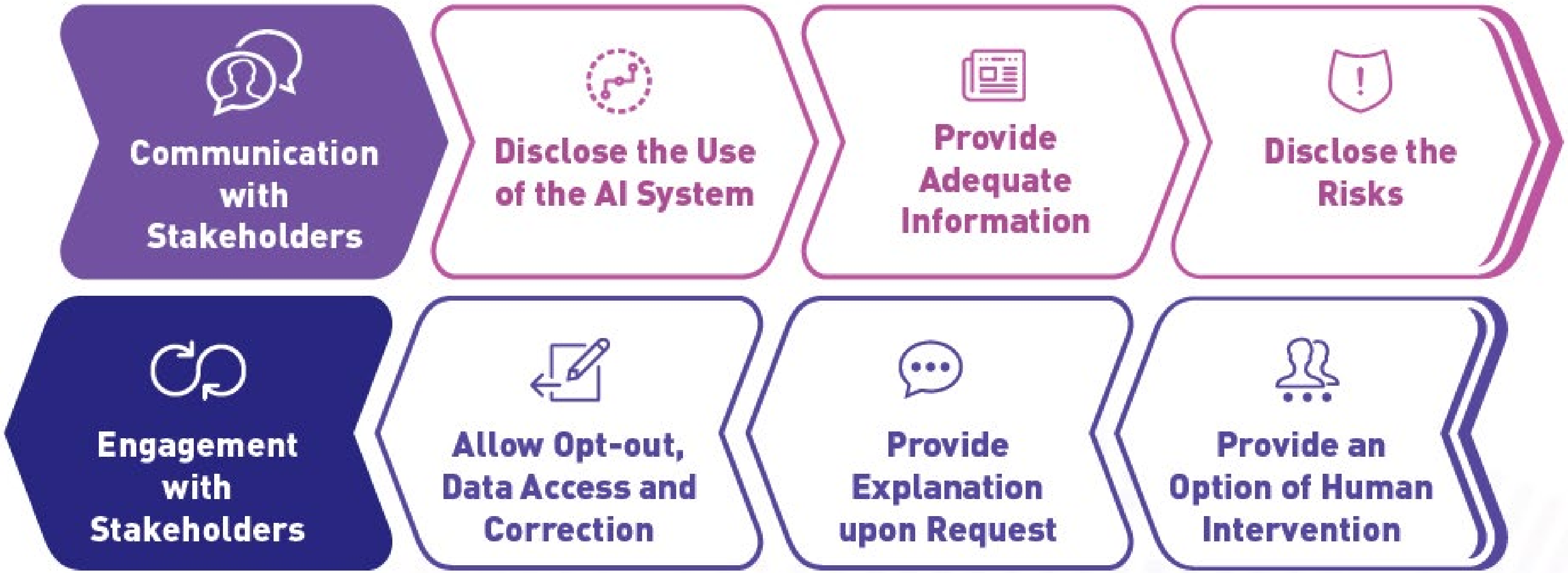
4 Containing an AI Incident

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

PCPD
H K

Contact Us

Hotline 2827 2827

Fax 2877 7026

Website www.pcpd.org.hk

Email communications@pcpd.org.hk

Address Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen’ s
Road East, Wanchai, Hong Kong

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

Follow us