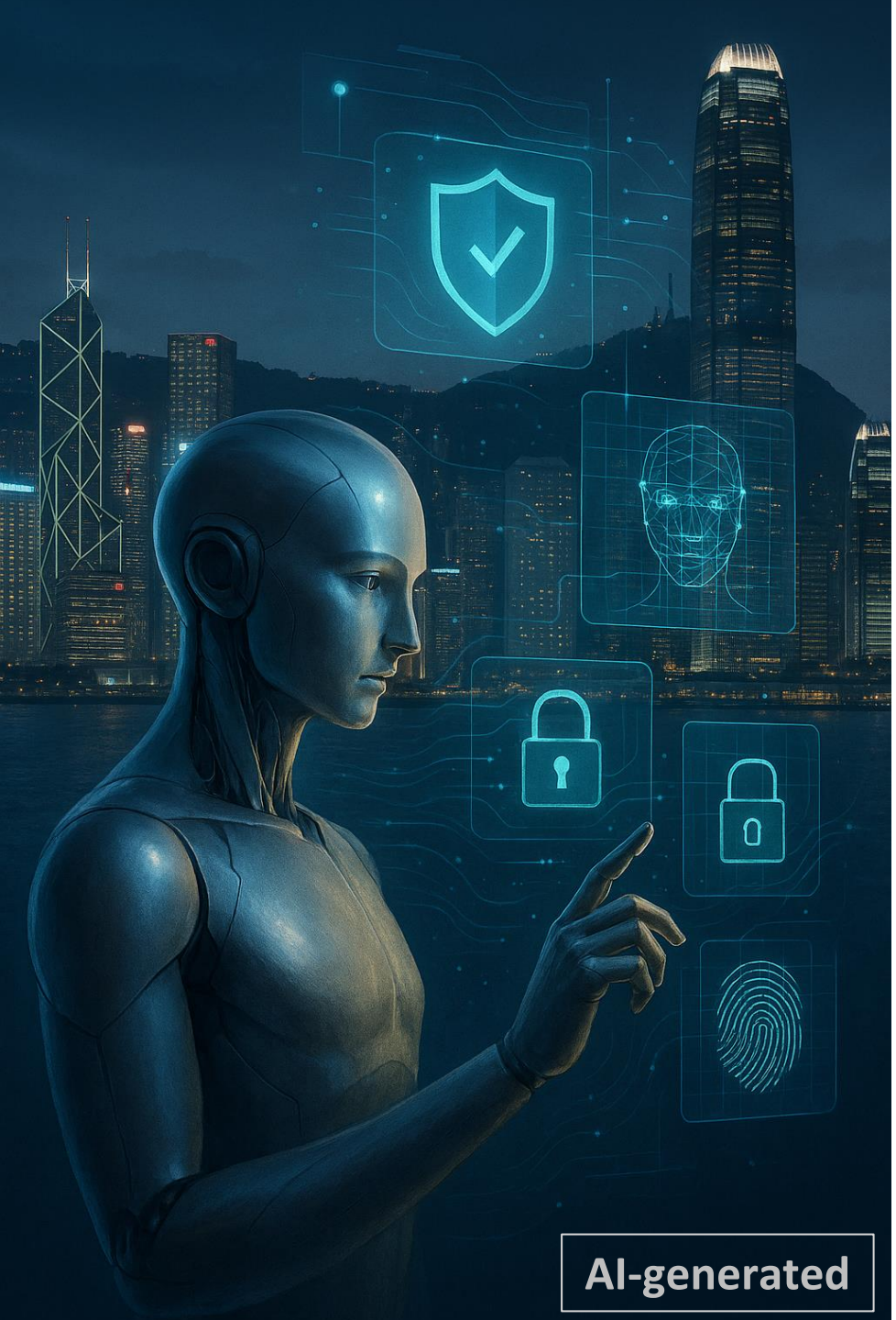


PCPD HK

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

Cyber Security Summit 2025

AI and the Next Chapter in Privacy Protection

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data

7 November 2025

2025 APEC Economic Leaders' Meeting

The Gyeongju Declaration recognsied the rapid advancement of AI

Background

AI security has become a common theme

International collaborations

AI SAFETY SUMMIT

Nov 2023

28 countries, including China, EU and the US, signed the **Bletchley Declaration**

United Nations

Mar 2024

United Nations General Assembly adopted its first international resolution on AI, encouraging the promotion of **"safe, secure and trustworthy" AI systems**

AI ACTION SUMMIT

Feb 2025

Around 60 countries and international organisations, including China, signed **"Statement on Inclusive and Sustainable Artificial Intelligence for People and the Planet"**

AI Security: an important aspect of national security in China

2023 "Global AI Governance Initiative"	Proposed principles such as **"people-centred, AI for good"**
2024 "AI Safety Governance Framework"	Set out comprehensive governance measures and technical measures to **guard against various risks posed by AI, including privacy risks**
2025 "Global AI Governance Action Plan"	Called for "**advancing the governance of AI safety**" and "[improving] data security and **personal information protection standards**"

Global Regulatory Developments

Artificial Intelligence Act (Aug 2024)

The Basic Act on the Development of Artificial Intelligence and Establishment of Foundation for Trust (effective Jan 2026)

- Measures for Labelling Content Generated by Artificial Intelligence (effective Sep 2025)
- Global AI Governance Action Plan (Jul 2025)
- 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)
- 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)

- No comprehensive AI legislation
- Sectoral approach

Joint statement on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI

International Collaboration

PCPD has collaborated with global counterparts in enhancing AI security

Co-chair of "Ethics and Data Protection in Artificial Intelligence Working Group" of Global Privacy Assembly

- PCPD **co-sponsored resolutions**

For example:

- **Meaningful Human Oversight of Decisions** Involving AI Systems (2025)
- **Collection, Use and Disclosure of Personal Data to Pre-Train, Train and Fine-Tune** AI Models (2025)

Co-chair of "International Enforcement Cooperation Working Group" of Global Privacy Assembly

- To **strengthen international collaboration** and **address privacy challenges brought by AI**
- In 2023 and 2024, **PCPD, together with 11 and 15 privacy or data protection authorities worldwide, issued joint statements to social media platforms on data scrapping**

Risks

The use of AI may pose multiple personal data privacy risks

Risk	Explanation	Illustration
Data Breach	If users input personal data into AI chatbots, such data may be **transferred to the service providers**, posing a risk of data breaches	An employee at a **Dutch clinic** was found to have entered the highly sensitive **medical data of patients into an AI chatbot** without good reasons, **violating the privacy rights** of the patients
Excessive data collection	AI applications tend to **collect and retain as much data as possible**, which includes personal data	**An AI developer reportedly scraped 300 billion words online** for model training
Use of data	AI developers may use **personal data** to **train systems** without the data **subjects' knowledge** or **consent**	A **tech company trained AI models with records of 1.6 million patients** without their prior consent or any "opt-out" option
Data accuracy	Even when AI systems contain **outdated or inaccurate personal data**, developers may be **unable to correct or delete it**	An AI chatbot **repeatedly gave the wrong birth date** for a **public figure**, and the developer noted they were **unable to correct the output** by amending the training data

Sources: AP; Fortune; ICO, BBC; CPO Magazine

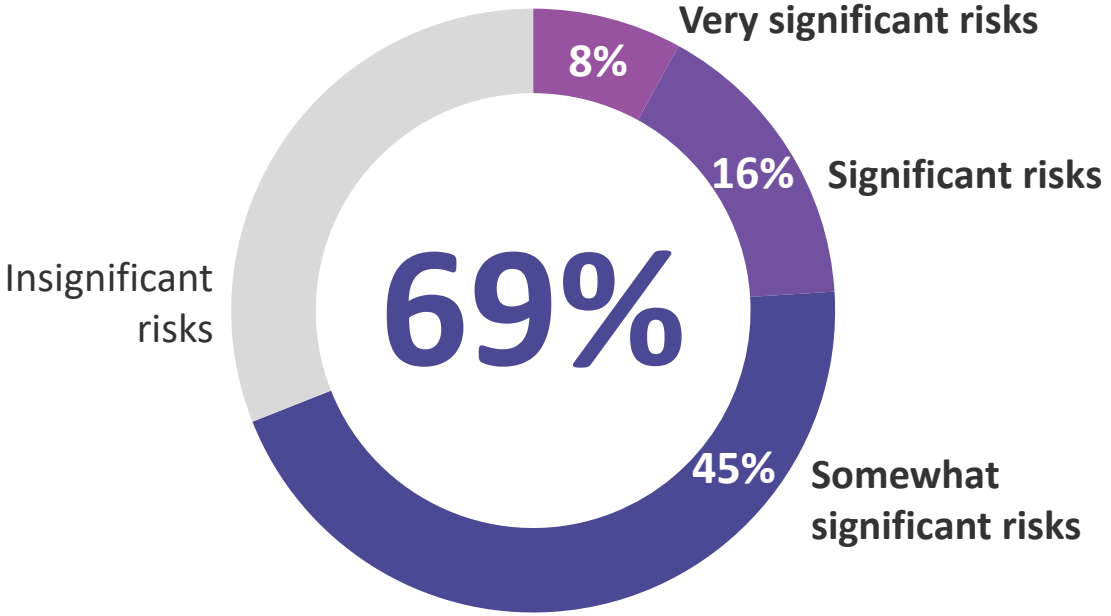
Risks

Enterprises consider AI as posing privacy risks

Most enterprises consider the use of AI in operations poses significant privacy risks

Perception of privacy risks of use of AI in operations

Hong Kong Enterprises, 2024

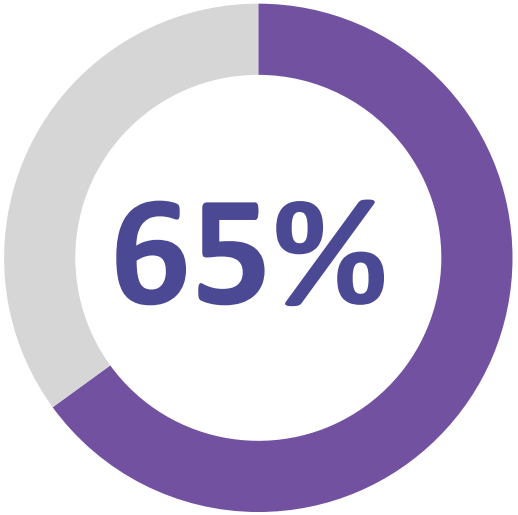


Source: PCPD & HKPC

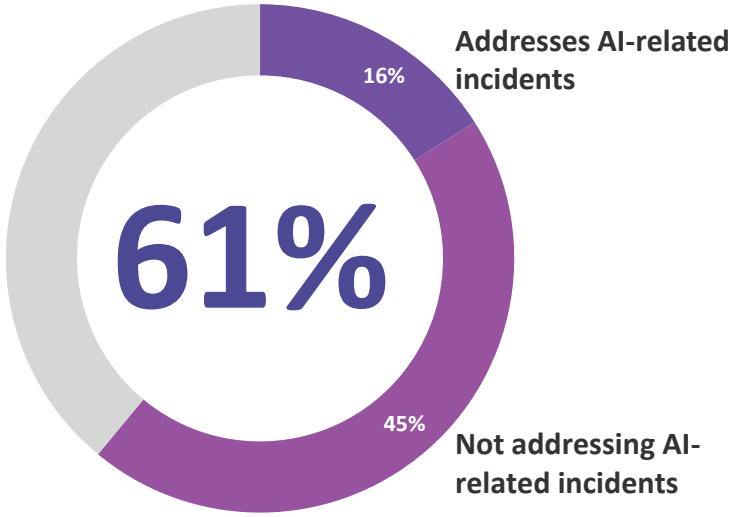
Measures

Organisations have implemented AI-related risk-mitigating measures

Enterprises using AI in operations (2024):



65% Implemented data security measures



61% have a data breach response plan, with 16% addressing AI-related incidents

Source: PCPD & HKPC

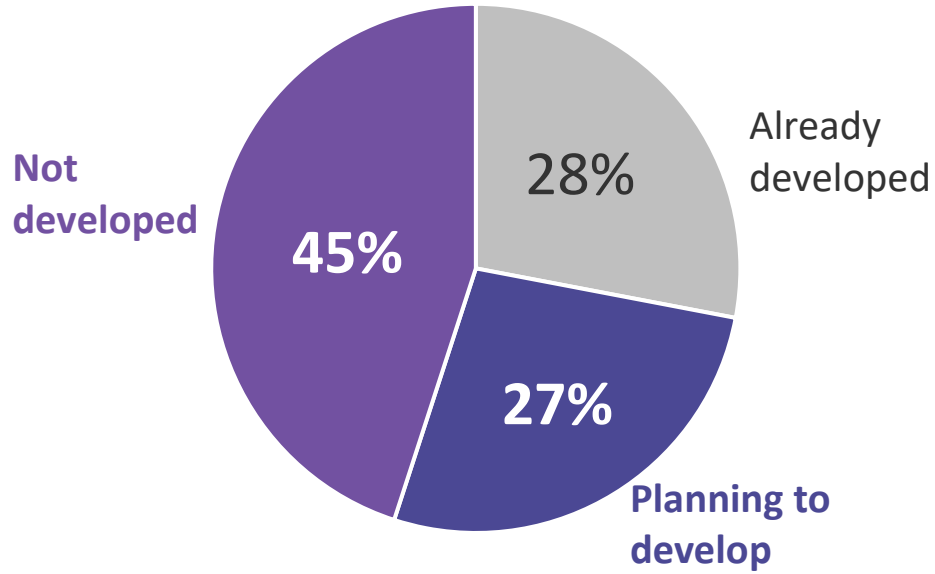
Enterprises' Readiness

Few enterprises formulate internal AI guidelines or offer training

Just around 30% of enterprises using AI have developed an AI security policy

Availability of an AI security policy

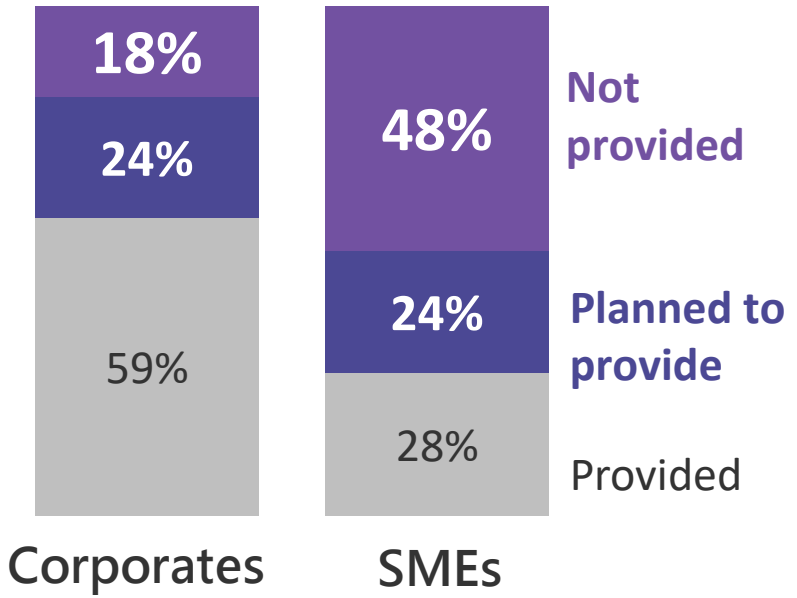
Hong Kong enterprises using AI in their operations, 2024



There is still room for increasing AI training, especially for SMEs

Provision of AI training to employees

Hong Kong enterprises using AI in their operations, 2024



Source: PCPD & HKPC

Compliance Checks

PCPD conducted compliance checks on the use of AI from 2023 to 2025

Aug 2023 to Feb 2024

PCPD conducted compliance checks on 28 local organisations to understand these organisations' practices in relation to the collection, use and processing of personal data in the development or use of AI, as well as AI governance of these organisations

Feb to May 2025

PCPD began a new round of compliance checks, which covered 60 local organisations across a wider range of sectors. In addition to the scope of the first round of compliance checks, PCPD also examined the organisations' implementation of the recommendations and best practices provided in the Model Framework

Results

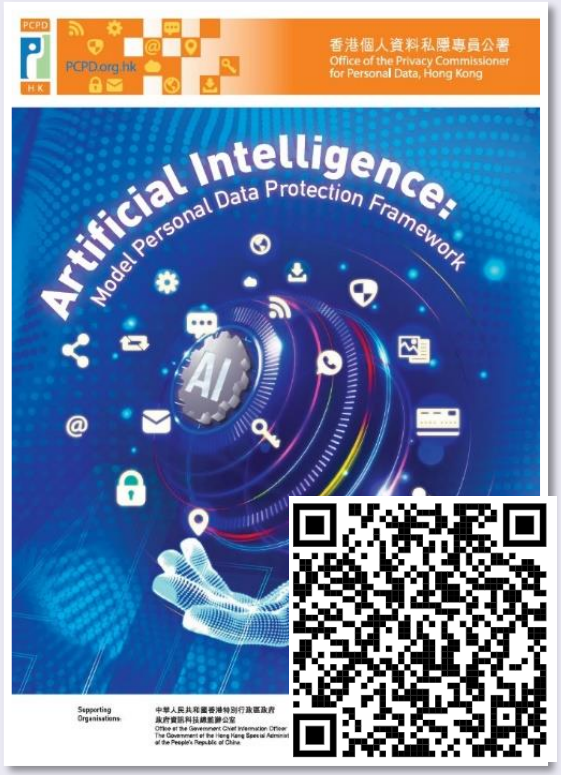
PCPD found no contravention of the Personal Data (Privacy) Ordinance (PDPO) during both compliance check processes

PCPD's Guidance

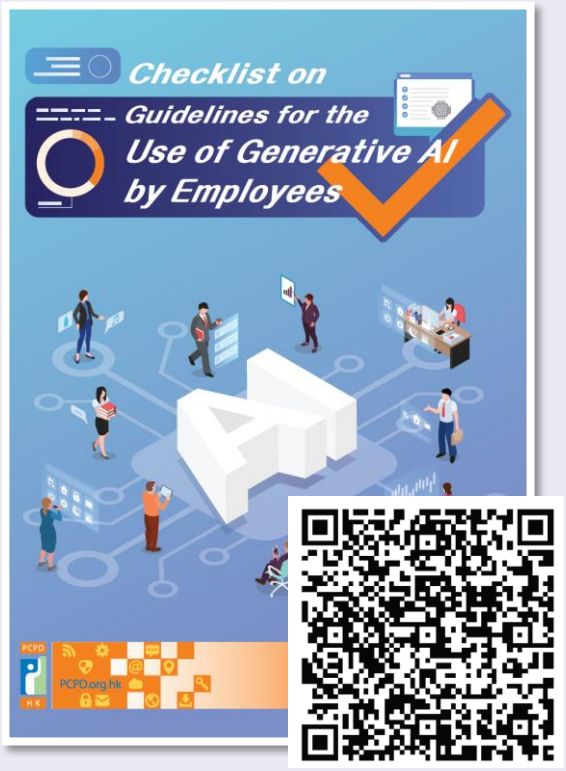
The PCPD has published different guidance in response to AI development

Organisations

Aug 2021



Jun 2024

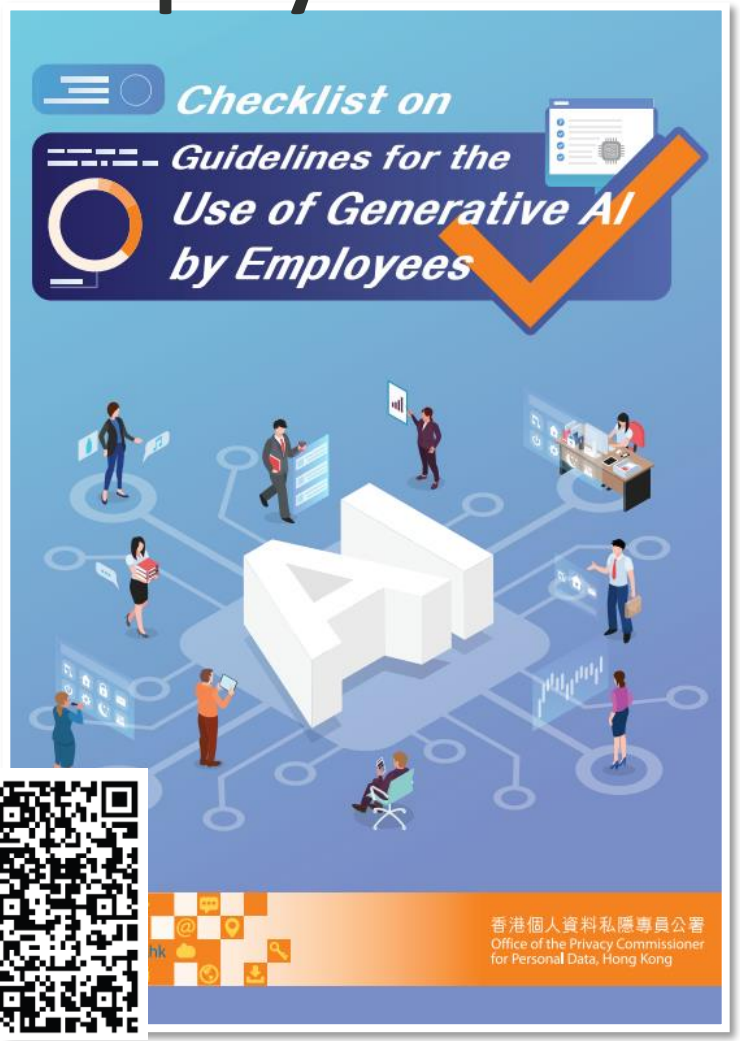


Mar 2025

Public

Sep 2023

Checklist on Guidelines for the Use of Generative AI by Employees



Objectives

To assist organisations in developing internal policies or guidelines on the use of Gen AI by employees at work while complying with the requirements of the PDPO

Features

Presented in the form of a checklist

As a matter of good practice, organisations should devise their own policies and guidelines in alignment with their values and mission

Recommended Coverage of Policies or Guidelines on the Use of Gen AI by Employees

01 Scope

02 Protection of personal data privacy

03 Lawful and ethical use and prevention of bias

04 Data security

05 Violations of policies or guidelines

01 Scope

Scope	Details
Permitted tools	**Specify the Gen AI tools and applications that are permitted within the organisation,** for example: • Publicly available Gen AI tools or applications • Internally developed Gen AI tools or applications
Permissible use	**Clearly specify the tasks or activities for which employees can use Gen AI tools,** for example: • Drafting • Summarising information • Creating textual, audio and/or visual content
Policy applicability	Specify if the policy applies to the **whole organisation**; **specific departments**; **specific ranks**; and/or **specific employees**

02 Protection of personal data privacy

Permissible types and amounts of input information

Provide clear instructions on:

✓ **The types and amounts of information that can be inputted into the Gen AI tools**

✗ **The types of information that cannot be inputted**

Permissible use of output information

Provide clear instructions on the **permissible purposes** for using the information (including personal data) generated by Gen AI tools, and whether, when and how such personal data should be anonymised before further use

Permissible storage of output information

Require that the information generated by Gen AI tools be stored according to the organisation's **information management policy** and deleted according to its **data retention policy**

Compliance with other relevant internal policies

Ensure that **the policy on the use of Gen AI is aligned with the organisation's other relevant internal policies**

03 Lawful and ethical use and prevention of bias

Unlawful activities

Specify that employees shall not use Gen AI tools for unlawful or harmful activities

Emphasise the importance of employees acting as human reviewers

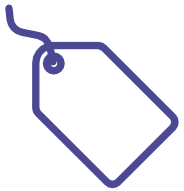
Accuracy and verification

Emphasise the need for employees to **verify the information provided by AI**

Prevention of bias and discrimination

Alert employees to the possibility that AI-generated output can be **biased and discriminatory**

Set out the **correction and reporting mechanisms**



Watermarking / labelling

Provide clear instructions on **when and how** AI-generated output should be **watermarked or labelled**

04 Data security

Permitted devices

Specify the **devices** on which employees are permitted to **access Gen AI tools**

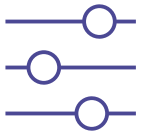
Permitted users

Specify the **permitted employees** of Gen AI tools

User credentials

Require employees to use **unique and strong passwords** along with **multi-factor authentication**

Security settings

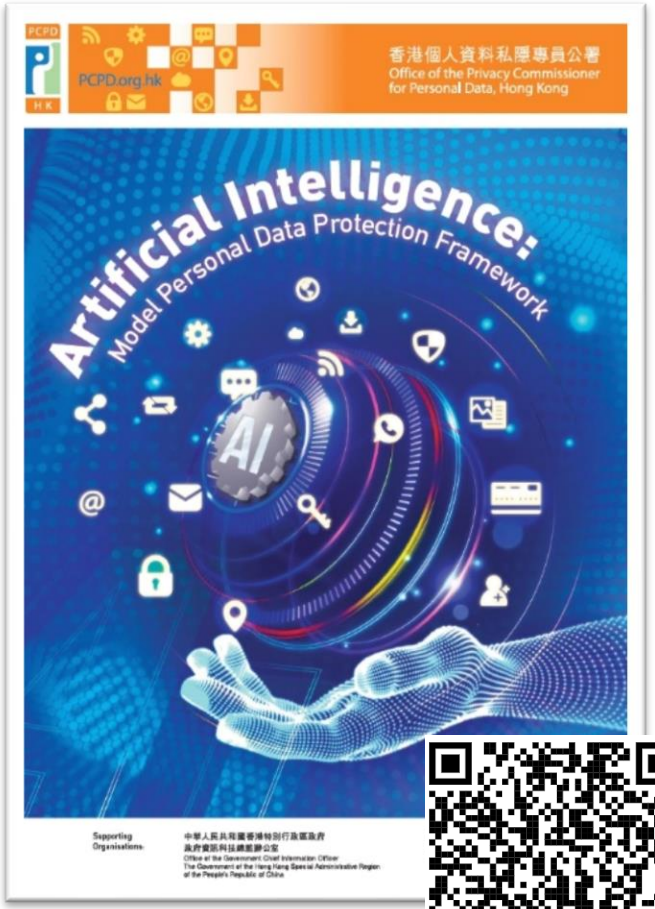


Require employees to maintain **stringent security settings**

Response to AI incident and data breach incident

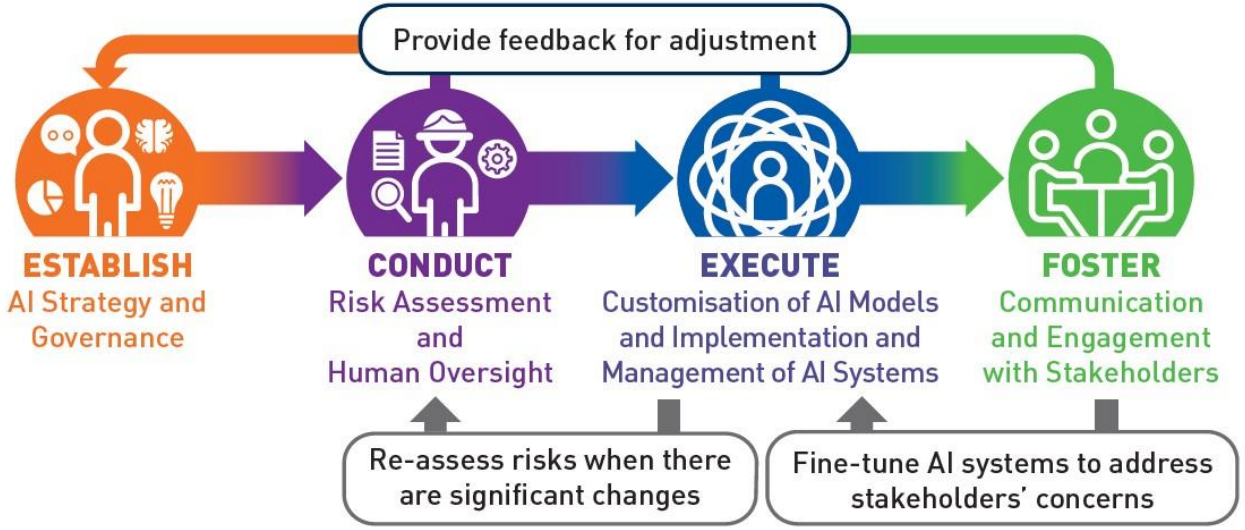
Require employees to **report AI incidents according to the organisation's AI Incident Response Plan**

Artificial Intelligence: Model Personal Data Protection Framework (Model Framework)



Issued in June 2024

Provide a set of recommendations on AI governance and best practices for organisations procuring, implementing and using any type of AI systems, including generative AI, that involve the protection of personal data privacy



Award for Model Framework

GovMedia Conference & Awards 2025

GOVMEDIA AWARDS 2025

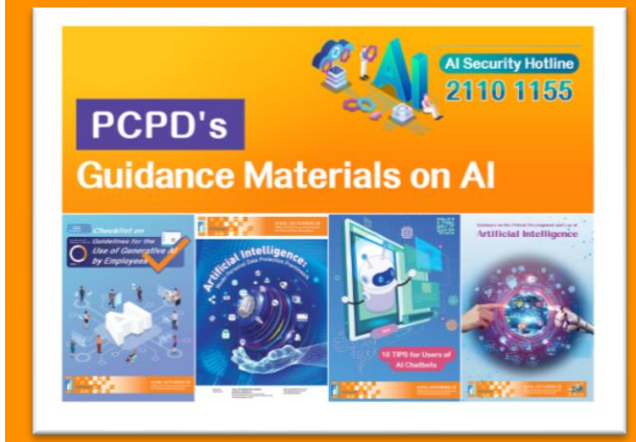
Hong Kong Public Sector
Initiative of the Year - Regulatory
Office of the Privacy Commissioner for Personal Data, Hong Kong, China

PCPD has won the "Hong Kong Public Sector Initiative of the Year – Regulatory" award in the Asia Pacific GovMedia Conference & Awards 2025 for the Model Framework

An awards programme organised by Asia Pacific news platform GovMedia to recognise public sector projects that are transforming the Asia Pacific region and making a global impact

The awards celebrate innovative solutions, excellence in governance and impactful projects that enhance public services and improve the lives of the public

Contact us



AI Thematic Webpage

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

Please Follow Us