The Hong Kong China Network Security Association
AI & Data Privacy Luncheon 2026

Data Privacy in the Age of AI

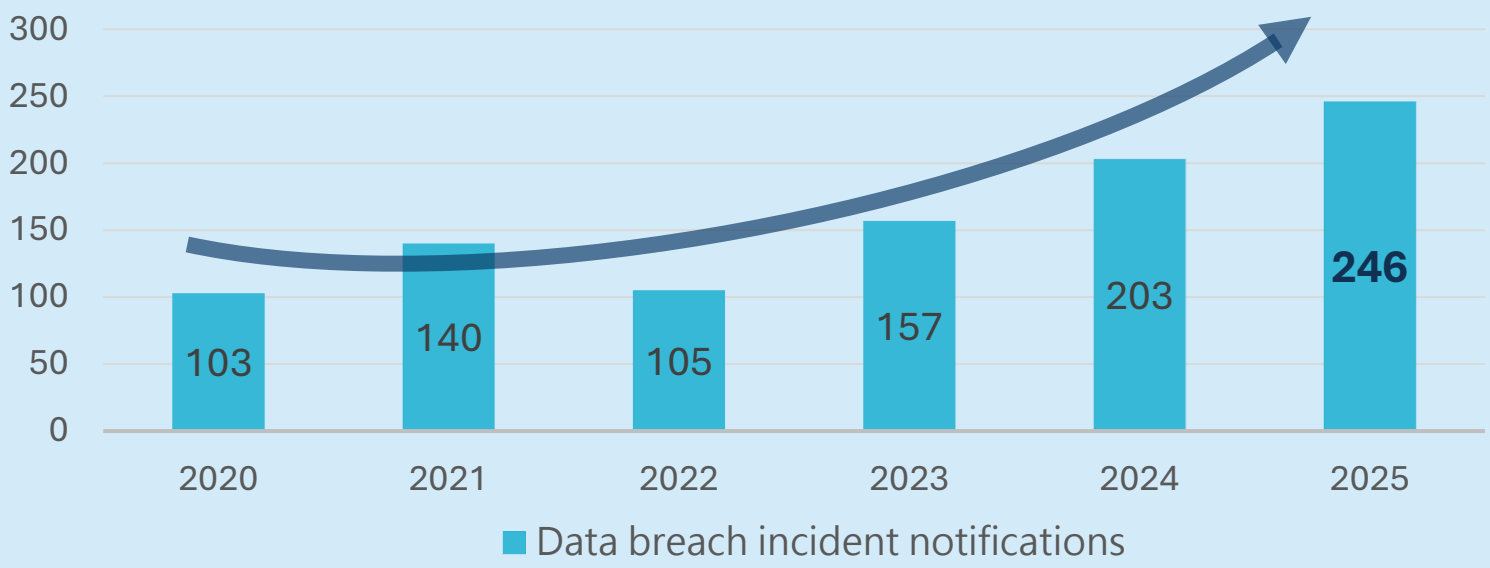
Ms Fiona LAI
Assistant Privacy Commissioner for Personal Data (Legal)
Office of the Privacy Commissioner for Personal Data

25 March 2026

守護私隱・改革創新
Protecting Privacy · Embracing Innovation

Rise in Data Breach Notifications

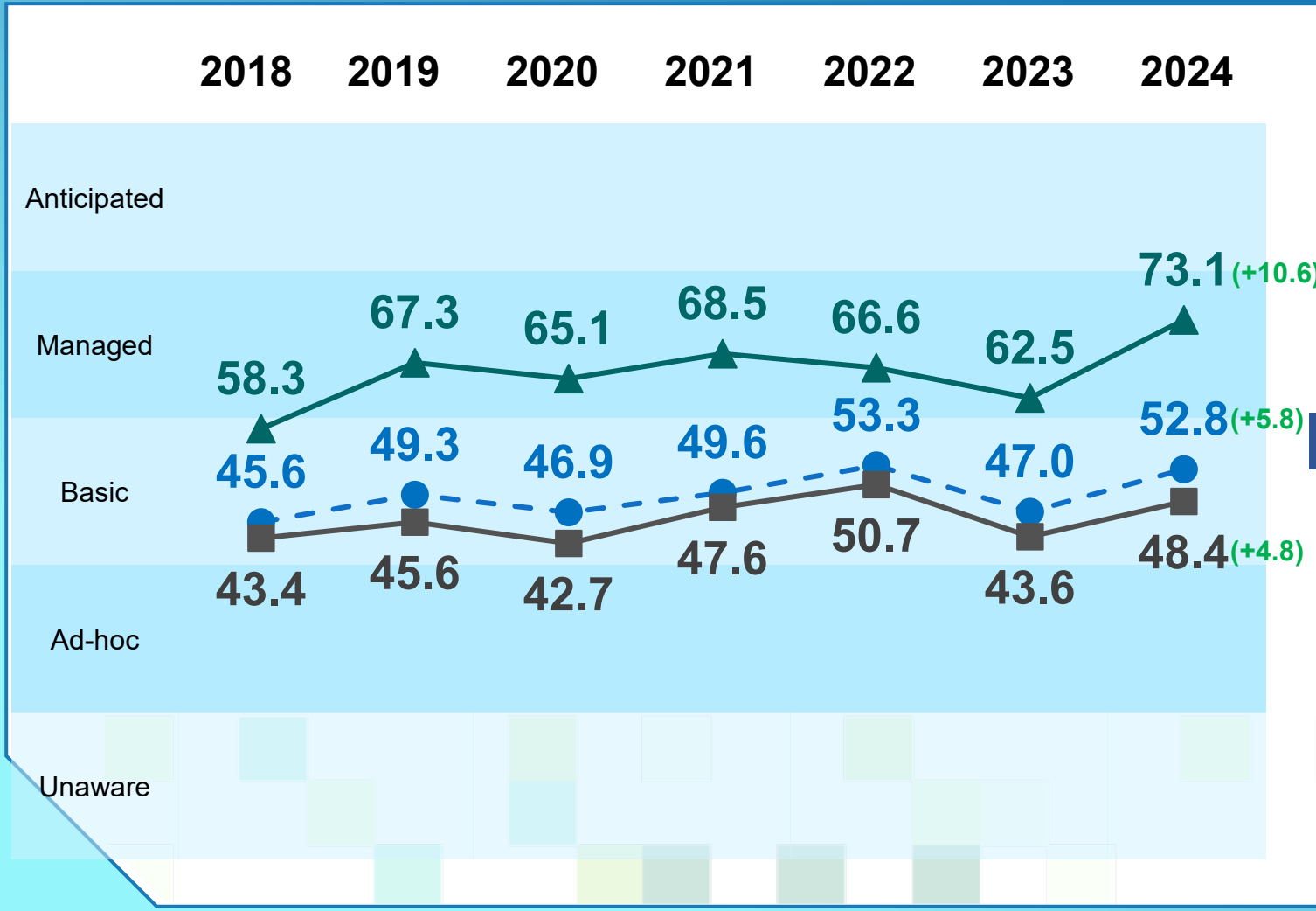
- A total of 246 data breach notifications received in 2025
  - ➢ Over 100% increase from the 103 incidents reported in 2020



Causes of Data Breach

1. Hacking
2. Loss of documents or portable devices
3. Inadvertent disclosure of personal data by email, post or fax
4. Employees' misconduct
5. System Misconfiguration
6. Others

Hong Kong Enterprise Cyber Security Readiness Index



Improving Cybersecurity readiness among enterprises

- Overall index rose by 5.8 points to 52.8 points in 2024
- Index for Corporates reached all-time high at 73.1 points

Enterprises took proactive steps to strengthen their cybersecurity

- 53% adopted cybersecurity risk assessments
- 60% conducted regular review on critical IT systems

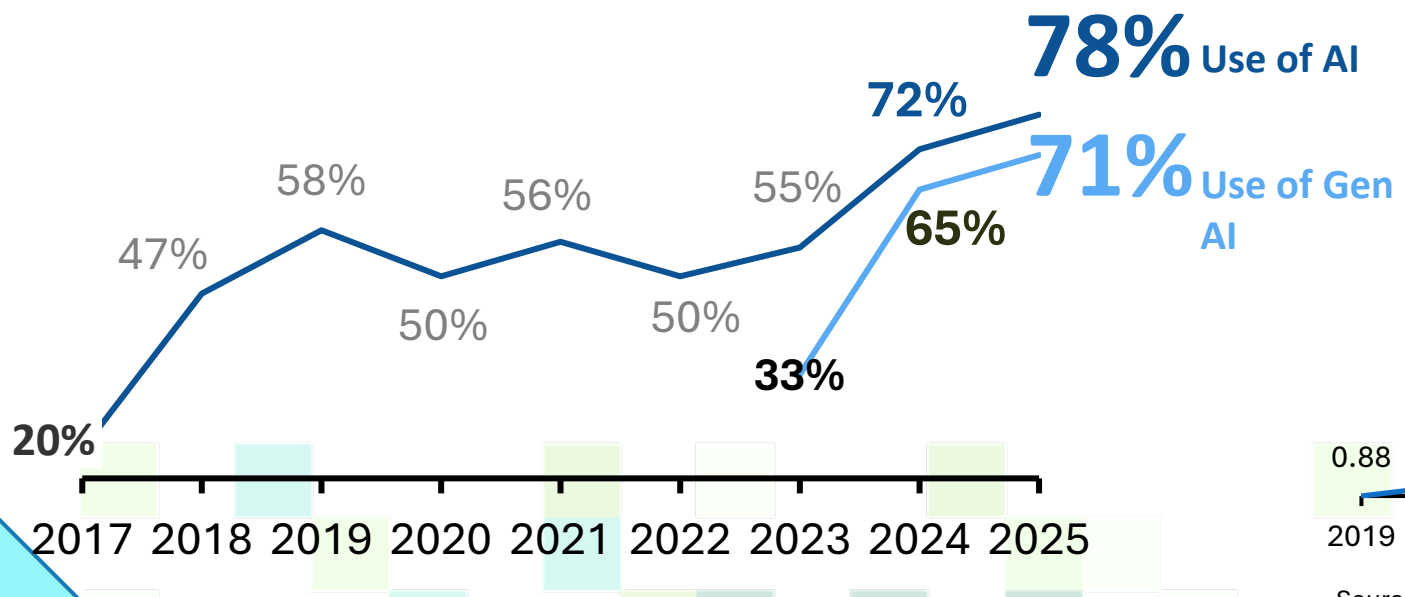
Rise in use of AI

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

Global AI (including gen AI) adoption rate has soared

Organisations that use AI in at least 1 business function

Organisations from >100 countries, 2017-2025

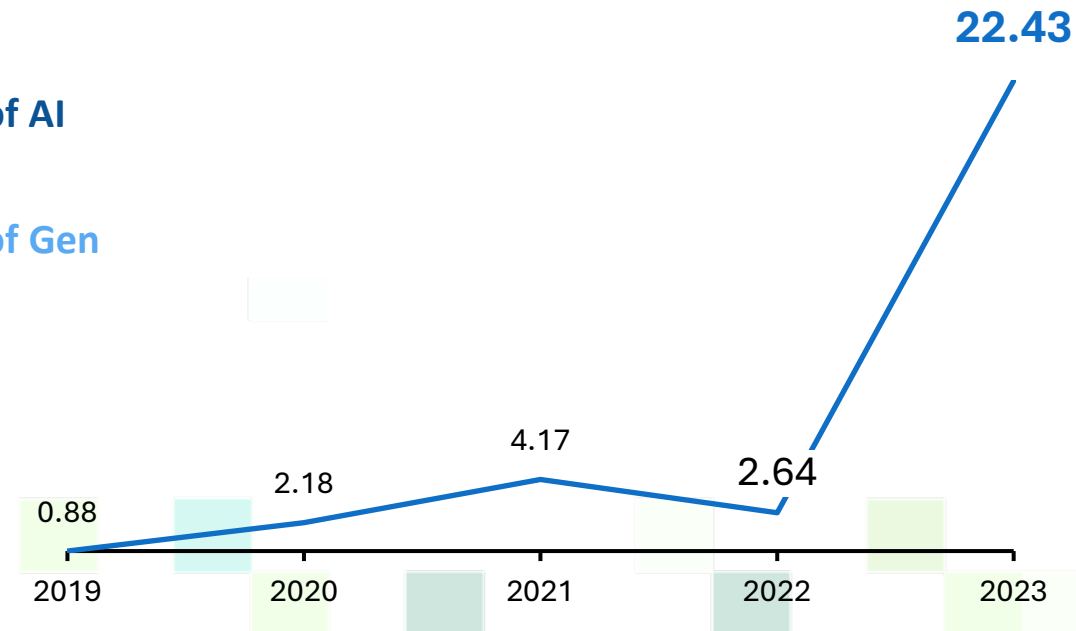


Source: McKinsey

Global investments in gen AI has surged

Private investment in gen AI

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



Source: Our World in Data

Local Context

Hong Kong embraces AI

HK is keen to grow its AI industry

- AI as a focus of HK's new **industrialisation**
- Building an AI **supercomputing centre**
- **14 research labs** under AIR@InnoHK
- Access to **mainland and international data** as HK's appeal

Businesses & employees keen to adopt AI

Integration of AI

Survey of 800 local companies, 2025

88%

Employees use AI in day-to-day work

45%

Employers recognise AI platforms for employees to use, yet…

54%

Employers do not have AI governance framework or policy

View towards AI Adoption

92%

Employers plan to introduce AI into workflows in the future

Source: HKPC

Individuals have used AI in work or life

Use of generative AI

Primary and secondary school students

95%

Have used generative AI before

Source: The Standard

Risks of AI

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 of AI

X could face UK ban over deepfakes, minister says

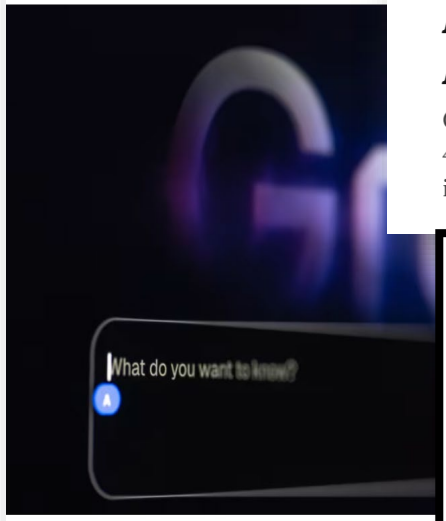
10 January 2026

Share Save

Musk's Grok blocked by Indonesia, Malaysia over sexualized images in world first

UPDATED JAN 13, 2026

By Lex Harvey



The chat window for chatbot Grok on a laptop on June 9, 202

Musk's Chatbot Flooded X With Millions of Sexualized Images in Days, New Estimates Show

Over nine days, Elon Musk's Grok chatbot generated and posted 4.4 million images, of which at least 41 percent were sexualized images of women.

Joint Statement on AI-Generated Imagery and the Protection of Privacy

23 February 2026

The co-signatories below are issuing this Joint Statement in response to serious concerns about artificial intelligence (AI) systems that generate realistic images and videos depicting identifiable individuals without their knowledge and consent.

While AI can bring meaningful benefits for individuals and society, recent developments - particularly AI image and video generation integrated into widely accessible social media platforms - have enabled the creation of non-consensual intimate imagery, defamatory depictions, and other harmful content featuring real individuals. We are especially concerned about potential harms to children and other vulnerable groups, such as cyber-bullying and/or exploitation.

Source: CNN; BBC; The New York Times

China Is Embracing OpenClaw, a New A.I. Agent, and the Governme Is Wary

Excitement about A.I. assistant tools is running into growin concerns about the security risks of software that operates autonomously on user's devices.

Listen · 6:34 min

Share full article

People sought help from engineers to install OpenClaw, an open-source A.I. assistant, in China last week. Adek Berry/Agence France-Presse — Getty Images

Chinese authorities warn against misuse of OpenClaw amid rising security risks of unauthorized information leaks; expert urges users to strictly manage access

By Sun Langchen

Published: Mar 03, 2026 01:58 PM

OpenClaw, an open-source AI agent Photo: VCG

Source: The New York Times; Global Times

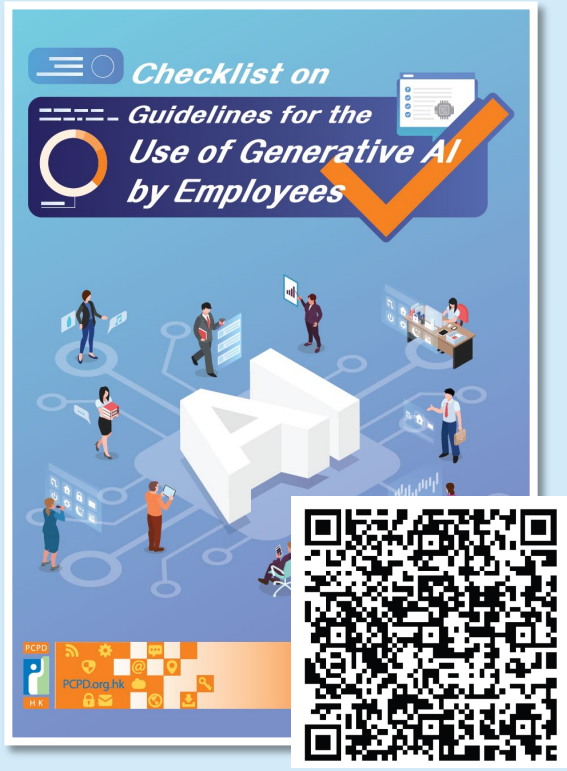
PCPD's Guidance

PCPD has published various guidance in response to AI developments

Organisations

Aug 2021

Jun 2024

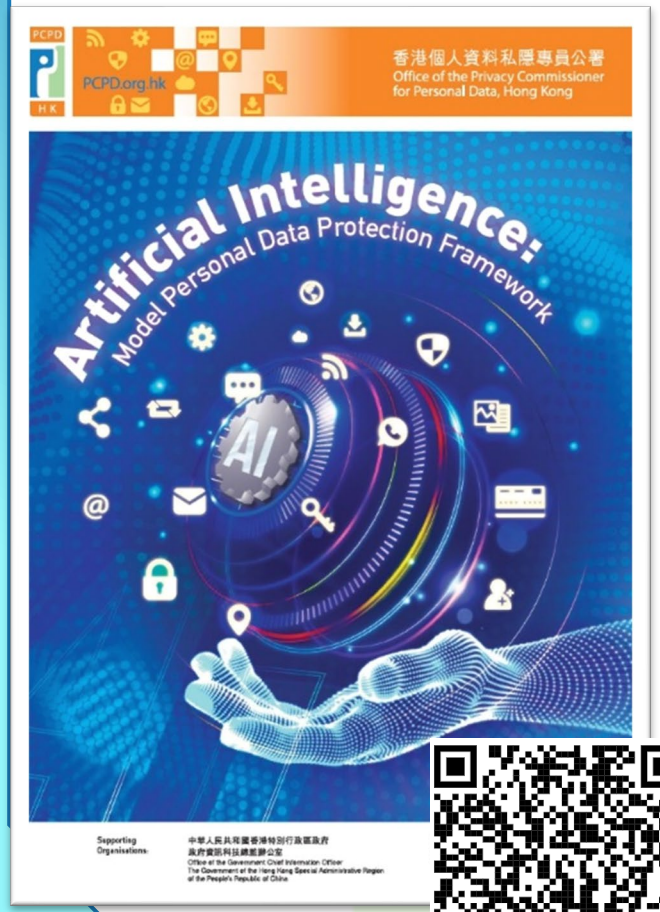


Mar 2025

Public

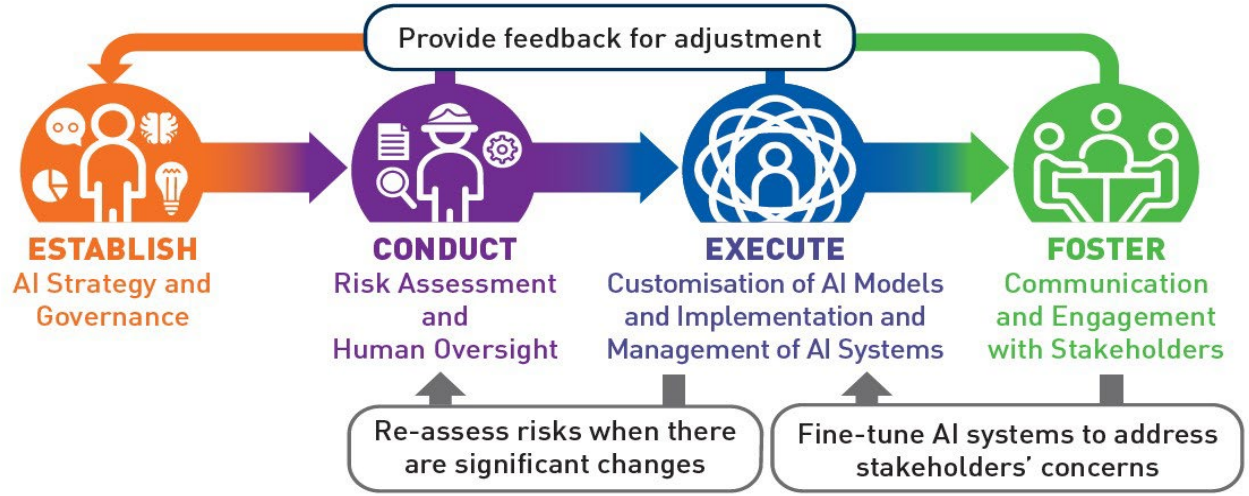
Sep 2023

Artificial Intelligence: Model Personal Data Protection 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**



Artificial Intelligence: Model Personal Data Protection Framework

ESTABLISH
AI Strategy and Governance

- **AI Strategy**
- **Governance Considerations**
- **Governance Structure**
- **Training and Awareness Raising**

CONDUCT
Risk Assessment and Human Oversight

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

Artificial Intelligence: Model Personal Data Protection Framework

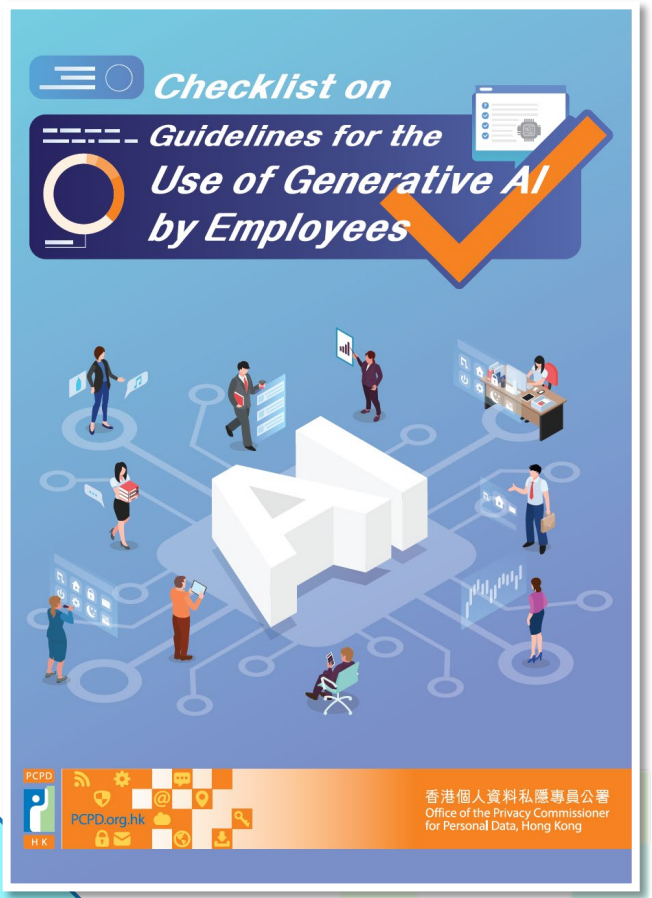
EXECUTE
Customisation of AI Models and Implementation and Management of AI Systems

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

FOSTER
Communication and Engagement with Stakeholders

- Information Provision
- Explainable AI
- Data Subject Rights and Feedback
- Language and Manner

Checklist on Guidelines for the Use of Generative AI by Employees



Issued in March 2025

Help organisations develop internal policies or guidelines for employees' use of GenAI at work while complying with the requirements of the PDPO

01 Scope

02 Protection of Personal Data Privacy

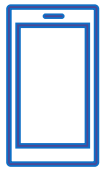
03 Lawful and Ethical Use and Prevention of Bias

04 Data Security

05 Violations of the policies or guidelines

04 Recommended Coverage of Policies or Guidelines on the Use of Gen AI by Employees – Data security

Permitted devices



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

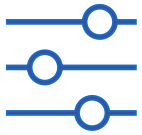
Permitted users

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**

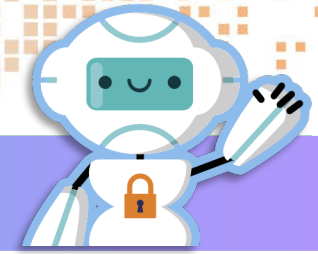
Response to AI incident and data breach incident

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

PCPD.org.hk

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

守護私隱・改革創新
Protecting Privacy・Embracing Innovation



Contact Us

Phone: 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.

Follow Us

私隱公署PCPD

香港个人资料私隐专员公署

Office of the Privacy Commissioner for Personal Data, Hong Kong