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

Navigating the Governance Challenge in the Digital Era

Key Governance Principles for Responsible AI

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data

30 September 2025

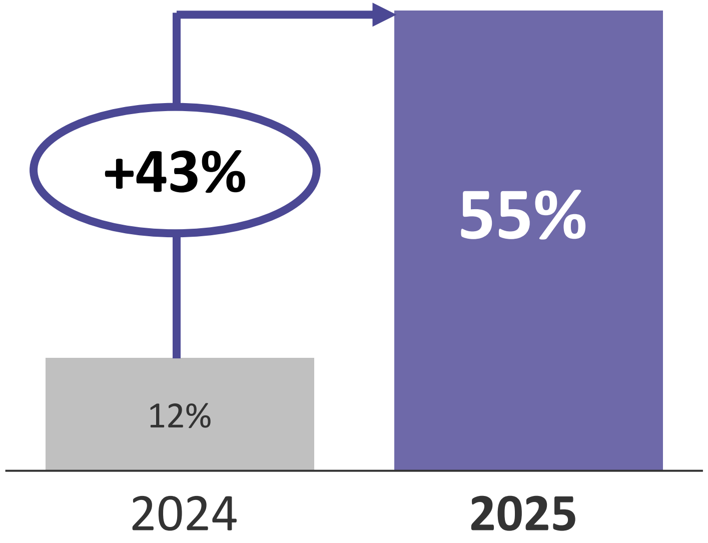
Statistics

Despite rising AI adoption, concerns remain

Global use of AI among non-profit organisations (NGOs) has soared

NGOs actively using or currently piloting AI

1229 NGOs

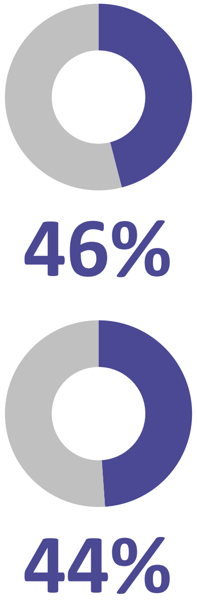


Source: Salesforce

NGOs' top concerns about AI are data-related

Top concerns about AI

1229 NGOs



Data privacy

Data security

Source: Salesforce

Examples

Many AI use cases have emerged in the social services sector

Service

Elderly

Safety

- AI-enabled bed exit sensors
- Anti-wandering systems

Menta health

- AI app for health

Children & Youth

Safety

- AI-powered surveillance cameras

Education

- Analysis of students with special educational needs

Family & Community

Integration

- App to help caregivers of SEN students

Emergency care

- ↗ AI flagging high-risk cases

Rehabilitation

Exercise

- App on mobile for personalised stroke rehabilitation exercises

Cross-service and Admin

Service Enhancement

- Narrative therapy on chatbots
- 24/7 AI chatbot for enquiries
- Platform for matching helpers with NGOs

Efficiency

- Meeting transcription and summary
- Case management

Source: HKCSS; Elderly[LegCo, ECare,]; C&Y [RTHK, Lenovo]; F&C [CUHK, i2hk]; Rehab [HKU]; Enhancement [J. of Social Work Practice, CIIF, HKCSS]; Efficiency [HKSPT, Community Care]

Risks

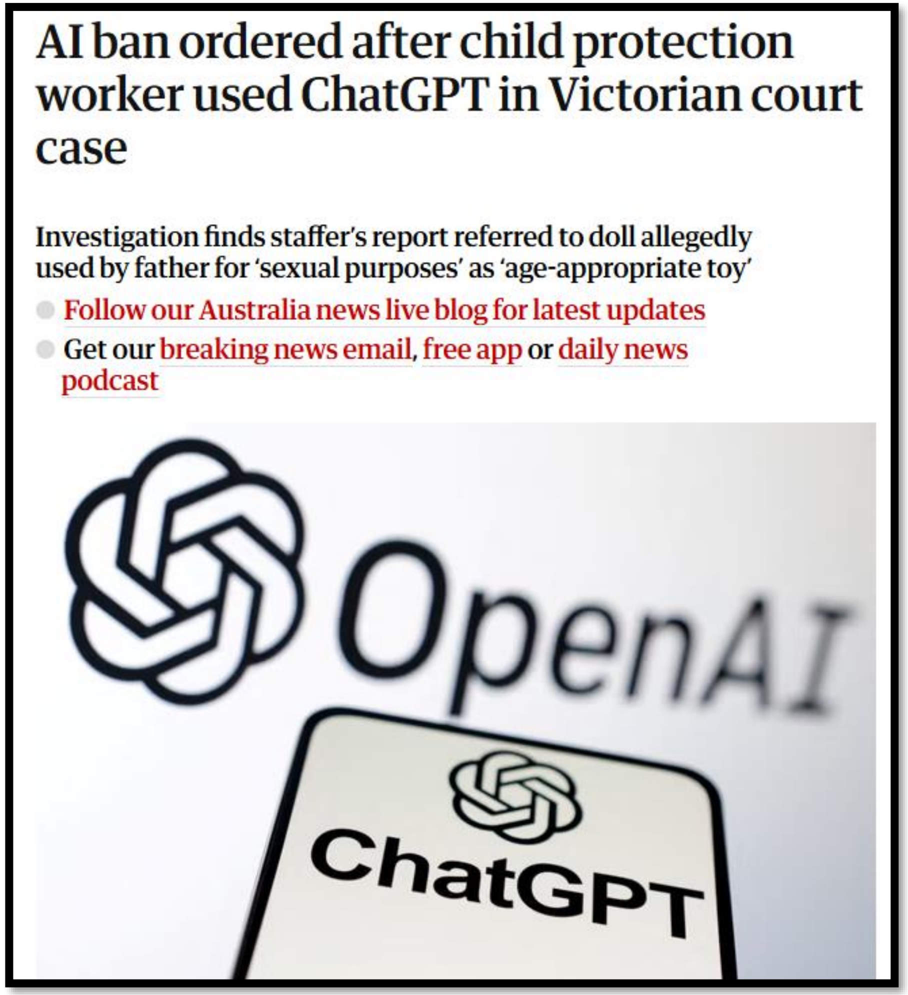
The use of AI may pose multiple personal data privacy risks

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

AI Incident

The use of an AI chatbot by a child protection worker led to serious issues



AI ban ordered after child protection worker used ChatGPT in Victorian court case

Investigation finds staffer's report referred to doll allegedly used by father for 'sexual purposes' as 'age-appropriate toy'

- Follow our Australia news live blog for latest updates
- Get our breaking news email, free app or daily news podcast

Source: The Guardian; Office of the Victorian Information Commissioner

The Incident

A child protection worker in Victoria, Australia submitted an AI-generated report to Children's Court

- The case involved a **child whose parents had been charged with sexual offences**
- **Personal information** of parents, carer and child **was inputted**

The relevant data protection authority found the following breaches:

- **Unauthorised disclosure** of personal information
- **Inaccuracy** of personal information in the Court's report

Compliance Checks

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

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

The Privacy Commissioner's Office has Completed Compliance Checks on 60 Organisations Regarding How the Use of Artificial Intelligence Affects Personal Data Privacy

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

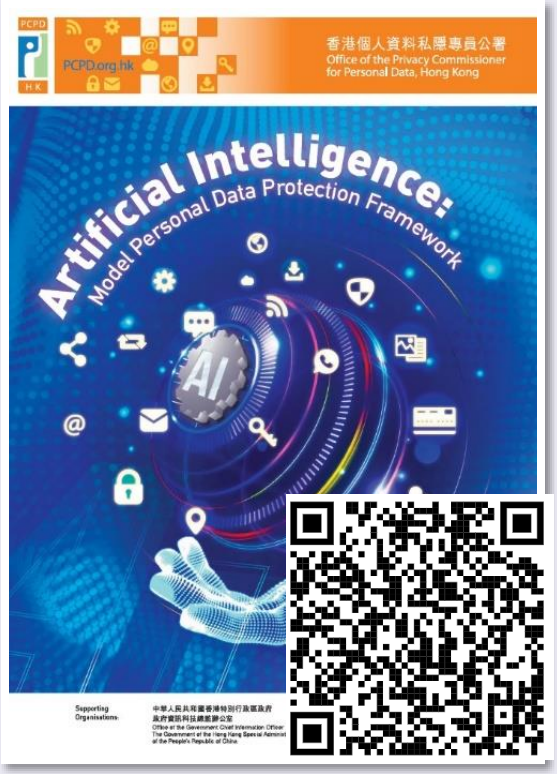
PCPD’s Guidance

The PCPD has published different guidance in response to AI development

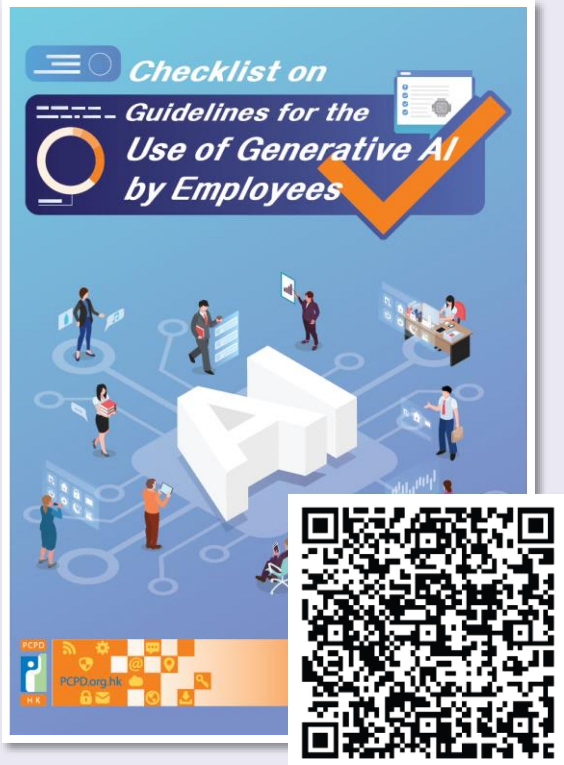
Organisations

Guidance on the Ethical Development and Use of Artificial Intelligence

Aug 2021


Artificial Intelligence: Model Personal Data Protection Framework

Jun 2024

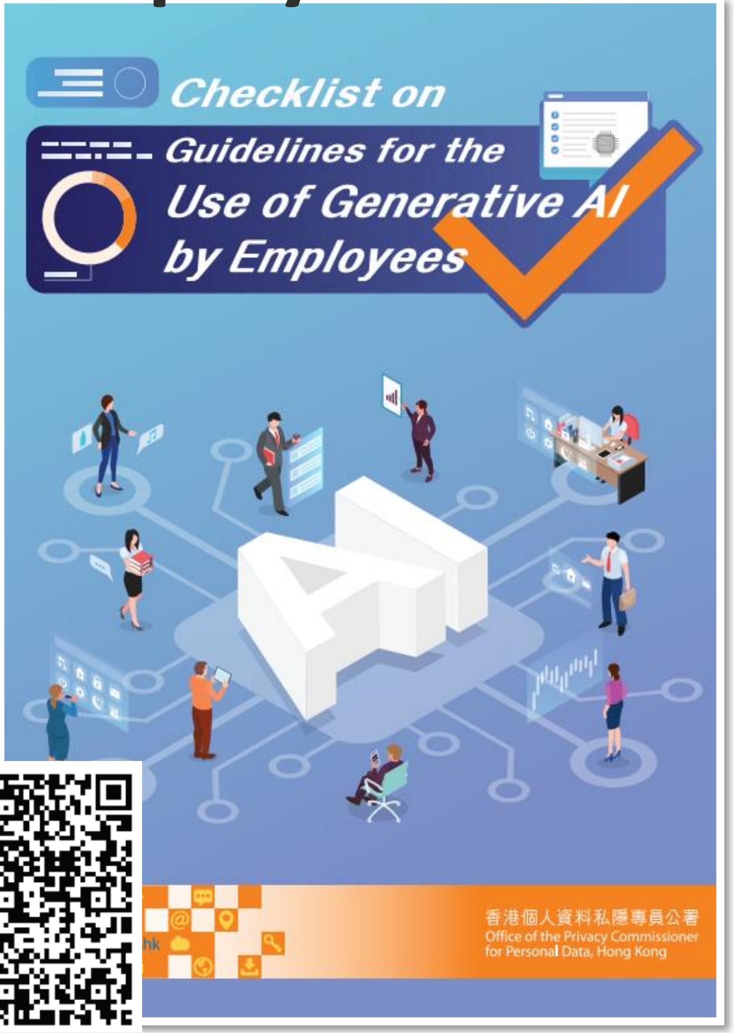

Checklist on Guidelines for the Use of Generative AI by Employees

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

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

✅ Benefits

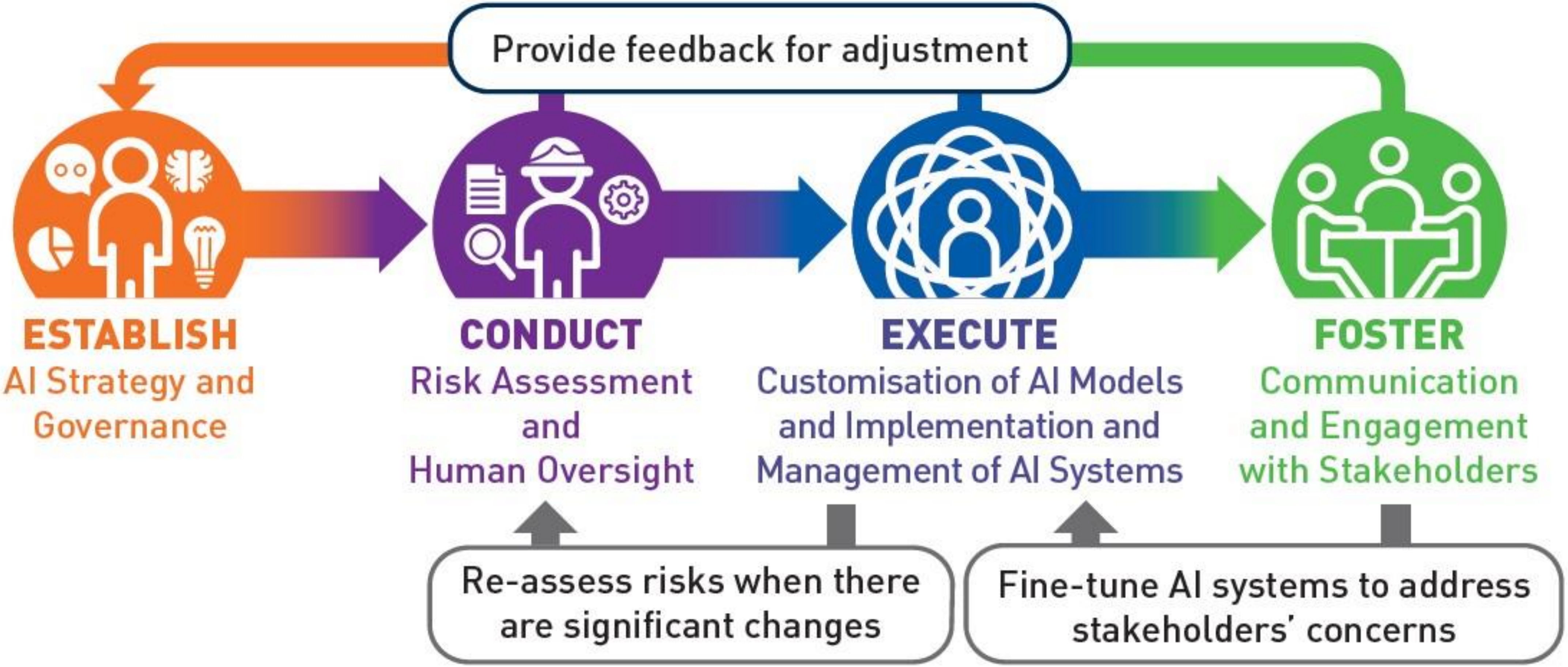
Assist organisations in complying with the requirements of the Personal Data (Privacy) Ordinance

Ensure AI Security

Increase competitiveness

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

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

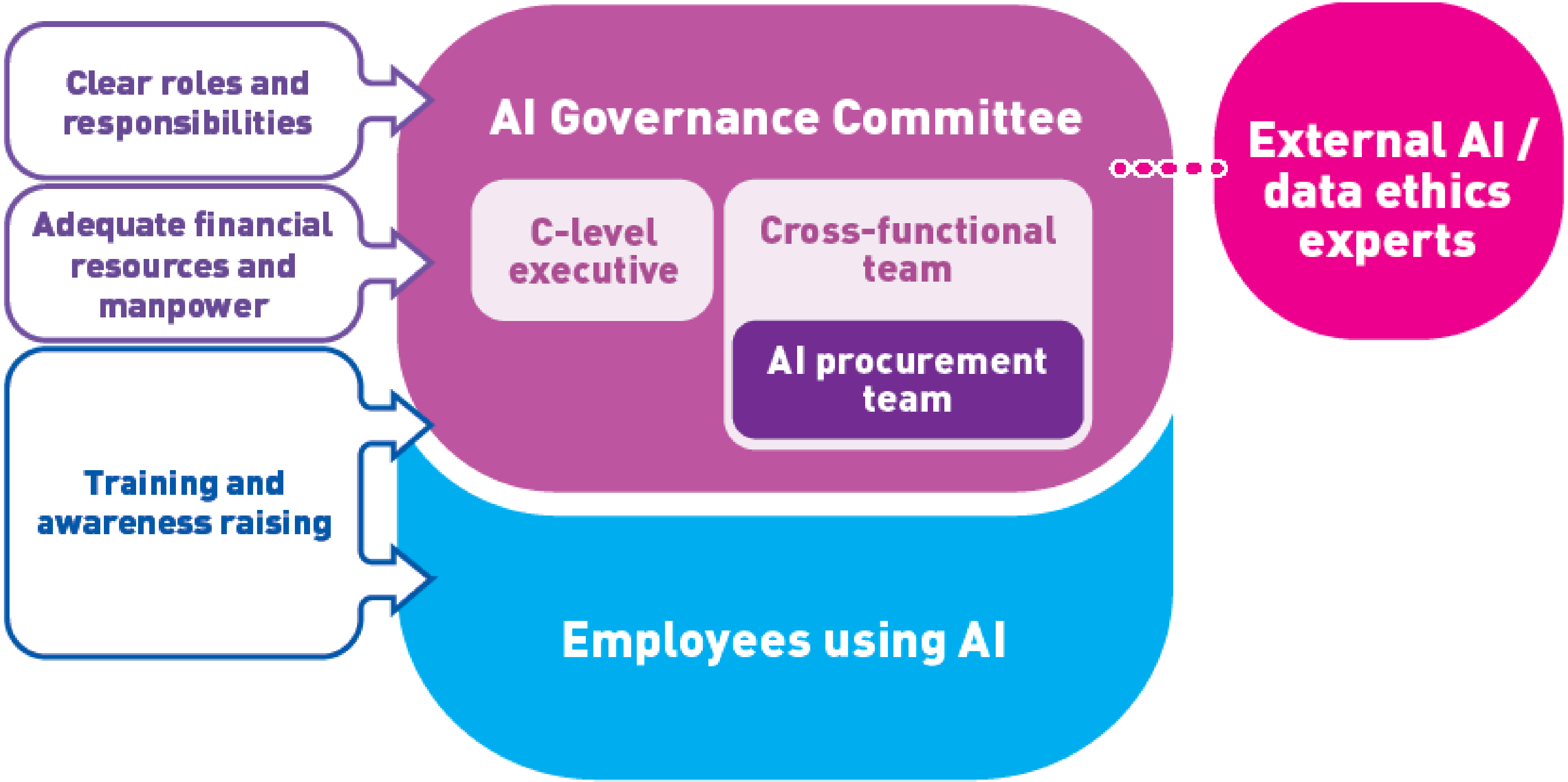
FOSTER
Communication and Engagement with Stakeholders

Re-assess risks when there are significant changes

Fine-tune AI systems to address stakeholders' concerns

Formulate AI Strategy and Governance

Governance structure



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

Risk-based approach to human oversight

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

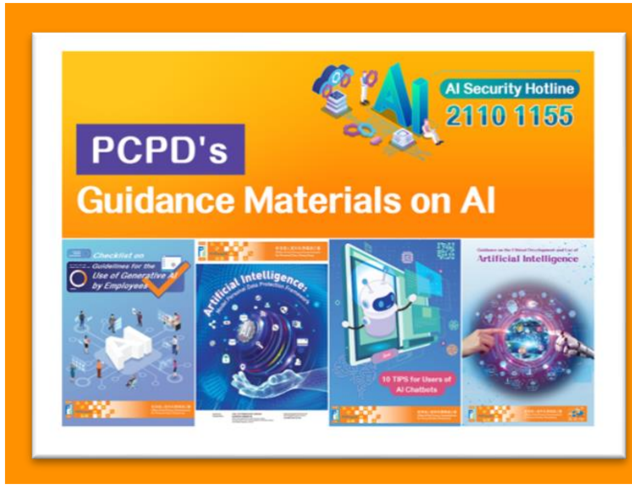
Data Preparation

Compliance, data minimisation, quality management, data handling

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

Process	Selected Recommendations
Data Preparation	Ensure compliance with privacy law Manage data quality Minimise the amount of personal data involved 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 Conduct periodic audits **Establish an AI Incident Response Plan** Consider incorporating review mechanisms as risk factors evolve

Contact us



AI Thematic Webpage

保障、尊重個人資料私隱

Protect, Respect Personal Data Privacy

Please Follow Us