

PCPD



H K

個人資料私隱專員公署

Office of the Privacy Commissioner for Personal Data

## AI and Privacy: Balancing Innovation with Ethical Use of Personal Data



Hong Kong International Computer Conference 2023  
28 September 2023

**Ada CHUNG Lai-ling**

Privacy Commissioner for Personal Data



PCPD



H K



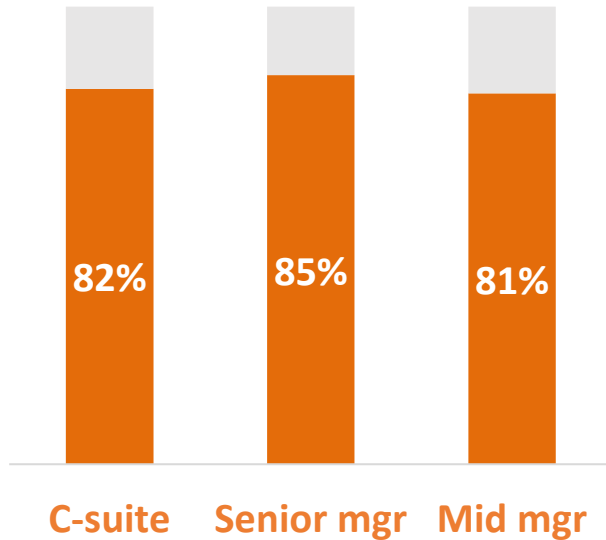
PCPD.org.hk

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

# Growing popularity of AI

## High AI use across levels

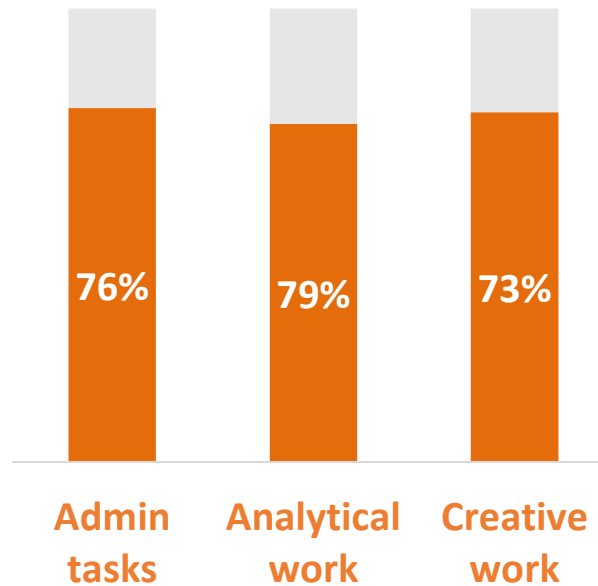
Exposure to generative AI tools  
% who tried at least once, by job title



Source: McKinsey (2023)

## Workers comfortable with AI

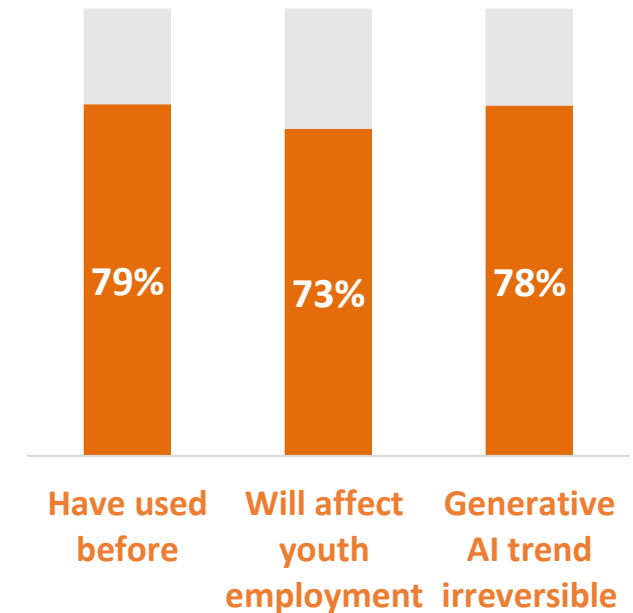
Views on AI in work  
Respondents comfortable with AI for...



Source: Microsoft (2023)

## Youth find AI impactful

Use/Views on generative AI  
Selected Hong Kong youth, age 15-34



Source: Youth I.D.E.A.S (2023)

# Deepfake

## Loan Scams

Hong Kong / Law and Crime

### Hong Kong police arrest 6 in crackdown on fraud syndicate using AI deepfake technology to apply for loans

- Force says case marks first known instance of scammers with stolen ID cards employing deepfake to fleece financial agencies
- Police remind public to be aware of signs of deepfakes in video calls, such as unnatural eye or mouth movements

- In August 2023, **Police arrested scammers** who used the **deepfake technology** of AI to **impersonate others in applying for loans online** with financial institutions
- A loan of **HK\$70,000** was approved





## Blackmailing

「眼見未為實」 港現深偽盜臉詐騙 事主疑直播App 聊天遭截圖 被「移花接木」色情片勒索



- In March 2023, a man was **threatened on a dating app to buy \$10,000 worth of game credits** with a video showing his **face superimposed on the body of a stranger engaged in sex acts**

# Privacy issues of AI

Issue	Explanation	Illustration
 <b>Excessive data collection</b>	AI applications tend to collect and retain as many data as possible, which includes personal data	OpenAI reportedly scraped 300 billion words online to train ChatGPT
 <b>Use of data</b>	AI models can be so advanced that people find it hard to understand how their personal data would be used	The “Black box” problem: users of AI are unable to know the internal logic of the AI systems
 <b>Identity re-identification</b>	Some AI models may be able to re-identify individuals’ identities by collecting & matching data from different sources	Studies show that it is possible to identify 93% of people in dataset with 60mn people using 4 pieces of data
 <b>Data accuracy</b>	Training AI models requires lots of data, and data quality & accuracy is an issue	AI may make incorrect analysis because of inaccurate data, which hampers decision-making

# AI's risks vis-à-vis Data Protection Principles (DPP)

DPP1

## PURPOSE AND MANNER OF COLLECTION

- Large amount of personal data collected
- Disclose little about collection

DPP2

## ACCURACY AND RETENTION

- Outdated/incorrect data becomes part of training data and is kept longer than necessary

DPP3

## USE OF DATA

- User conversations become new training data and may be reproduced for another purpose

DPP4

## DATA SECURITY

- Security risks of storing large amount of conversations

DPP5

## OPENESS AND TRANSPARENCY

- Data subjects are not fully informed of what personal data is held or how personal data is used

DPP6

## ACCESS AND CORRECTION

- Outdated/incorrect data that is part of training data is hard to be accessed or corrected



# Laws and regulations

## Published

国家互联网信息办公室  
中华人民共和国国家发展和改革委员会  
中华人民共和国教育部  
中华人民共和国科学技术部  
中华人民共和国工业和信息化部  
中华人民共和国公安部  
国家广播电视总局

令  
第15号

《生成式人工智能服务管理暂行办法》已经2023年5月23日国家互联网信息办公室2023年第12次室务会会议审议通过，并经国家发展和改革委员会、教育部、科学技术部、工业和信息化部、公安部、国家广播电视总局同意，现予公布，自2023年8月15日起施行。

国家互联网信息办公室主任 庄荣文  
国家发展和改革委员会主任 郑栅洁  
教育部部长 怀进鹏  
科学技术部部长 王志刚  
工业和信息化部部长 金壮龙  
公安部部长 王小洪  
国家广播电视总局局长 曹淑敏  
2023年7月10日

**MAINLAND CHINA: Interim Measures for the Management of Generative Artificial Intelligence Services (Aug 2023)**

## Proposed



A pro-innovation approach to AI regulation

**UK: White Paper on Pro-Innovation Approach to AI regulation**



**CANADA: Artificial Intelligence and Data Act**



**EU: Artificial Intelligence Act**

# PCPD's guidance

## Specifically for AI

1 Ethical Development and Use of AI (Aug 2021)

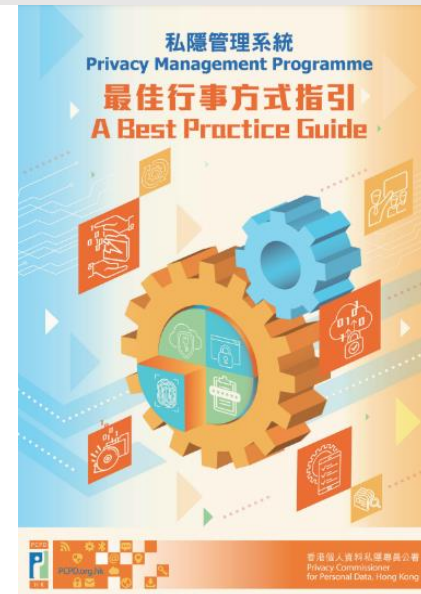


2 Tips on AI Chatbots (Sep 2023)

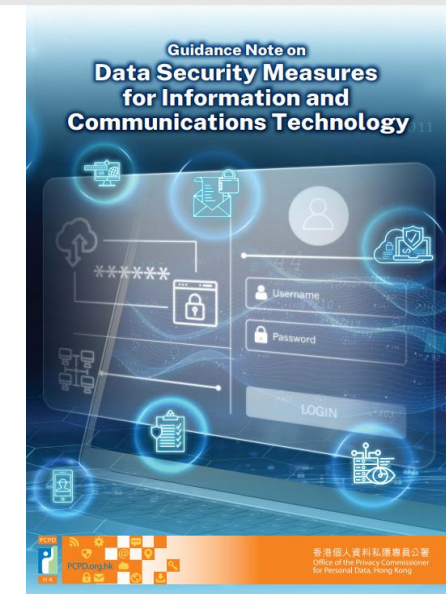


## Applicable to AI

3 Privacy Management Programme (PMP) (revised Mar 2019)



4 Data Security (Aug 2022)



# PCPD's guidance

## Specifically for AI

1 Ethical Development and Use of AI (Aug 2021)



2 Tips on AI Chatbots (Sep 2023)

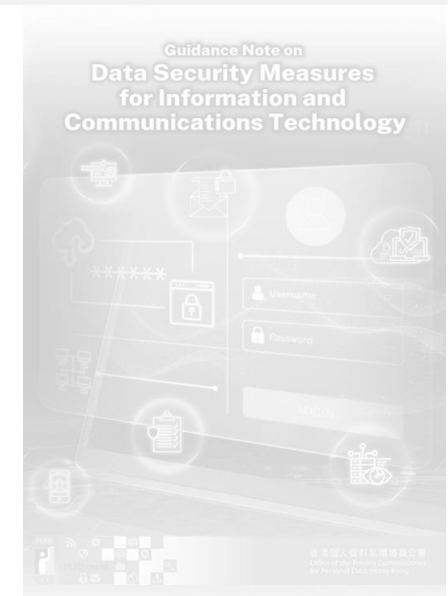


## Applicable to AI

3 Privacy Management Programme (PMP) (revised Mar 2019)









4 Data Security (Aug 2022)





# International efforts on promoting ethical AI

Jan 2019 – Aug 2021

- Jan 2019  **SINGAPORE:** Model Artificial Intelligence Governance Framework
- Mar 2019  **JAPAN:** Social Principles of Human-Centric AI
- Apr 2019  **EUROPEAN COMMISSION:** Ethics Guidelines for Trustworthy AI
- May 2019  **OECD:** Recommendation of the Council on Artificial Intelligence
- Aug 2021**  **HONG KONG's PCPD:** Guidance on the Ethical Development and Use of AI
- Aug 2021  **HONG KONG's OGCI:** Ethical AI Framework

Sep 2021 – Aug 2023

- Sep 2021  **MAINLAND CHINA:** Guidance on the Ethics of the New Generation AI
- Nov 2021  **UNESCO:** Recommendation on the Ethics of AI
- Mar 2022  **THAILAND:** Ethical Guidelines for AI
- Sep 2022  **FRANCE:** AI: Ensuring GDPR Compliance
- Mar 2023  **UK:** Guidance on AI and Data Protection (Updated)
- Aug 2023  **SOUTH KOREA:** Policy Direction for Safe Usage of Personal Data in the Age of AI

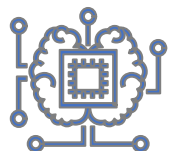
# 3 areas of our guide on AI

## Objectives



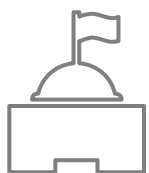
For business

Enable organisations to develop and use AI in **compliance with PDPO requirements**



For economy

Facilitate **healthy development and use of AI** in Hong Kong



For society

Facilitate HK to become an **innovation and technology (I&T) hub** as part of the **Greater Bay Area**

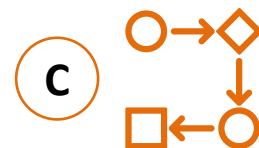
## Guidance



**3 Data Stewardship Values**



**7 Ethical Principles for AI**



**4-Step Practice Guide**

# 3 Data Stewardship Values



## BEING RESPECTFUL (尊重)

- Emphasise **rights, interests & reasonable expectations** of **stakeholders**
- Individual **treated ethically**, not piece of data



## BEING BENEFICIAL (互惠)

- The need to **benefit stakeholders**
- Not just those directly affected but also **wider community**
- **Prevent/minimise harm**



## BEING FAIR (公平)

- **Fair process & fair results**
- **Avoid bias & discrimination**
- **Justify differential treatments**

# 7 Ethical Principles for AI

## 1. Accountability

Organisations should:

- Be responsible & able to justify actions
- Have measures to assess & address AI risks



## 2. Human Oversight

- Human involvement level ~ risks & impacts
  - Risk-based approach



## 3. Transparency & interpretability

- Disclose use of AI & data privacy practices
  - Improve interpretability of automated & AI-assisted decisions



## 4. Data Privacy

- Put effective data governance in place
  - Process and protect personal data in accordance with PDPO



## 5. Fairness

- Avoid bias & discrimination



## 6. Beneficial AI

- Provide benefits
- Minimise harm to stakeholders



## 7. Reliability, Robustness & Security

- Ensure reliable AI operation
- Resilient to errors
- Protected from attacks with contingency plans



# 4-Step Practice Guide



**1. ESTABLISH**  
AI Strategy &  
Governance



**2. CONDUCT**  
Risk Assessment  
and Human  
Oversight



**3. EXECUTE**  
Development of  
AI Models &  
Management of  
AI Systems



**4. FOSTER**  
Communication  
with  
Stakeholders

Re-assess risks when  
there are significant  
changes

Fine-tune AI systems to  
address stakeholders'  
concerns

# Checklist for self-assessment

## APPENDIX A - Self-assessment Checklist

### AI STRATEGY AND GOVERNANCE

Question	Answer (Yes/No)	Further actions required
1 Has your organisation formulated an AI strategy before the development and use of AI?		
2 Did your organisation set up internal policies and procedures specific to the ethical design, development and use of AI?		
3 Did your organisation establish an AI governance committee (or a similar body) that would oversee the life cycle of the AI system, from its development, use to termination?		
4 Does the AI governance committee (or a similar body) have: <ul style="list-style-type: none"> <li>Members from different disciplines and departments to collaborate in AI development and use?</li> <li>A C-level executive (or management in a similar role) to oversee its operation?</li> </ul>		
5 Did your organisation set out clear roles and responsibilities for the personnel involved in the development and use of AI?		
6 Has your organisation set aside adequate resources in terms of finance and manpower for the development and use of AI?		
7 Has your organisation provided training to the personnel involved in the development and use of AI that is relevant to their respective roles?		
8 Has your organisation arranged regular awareness-raising exercises to the use of AI with all relevant personnel?		

### RISK ASSESSMENT AND HUMAN OVERSIGHT

Question	Answer (Yes/No)	Further actions required
1 Did your organisation conduct a risk assessment before the development and use of AI?		
2 Did the risk assessment of your organisation take into account personal data privacy risks and other ethical impact of the AI system?		
3 Were the risk assessment results reviewed and endorsed by the AI governance committee (or a similar body)?		
4 Has your organisation put in place an appropriate level of human oversight and other mitigation measures for the AI system, taking into account the risk profile of the AI system?		

### DEVELOPMENT OF AI MODELS AND MANAGEMENT OF AI SYSTEMS

Question	Answer (Yes/No)	Further actions required
<b>Preparation of Data</b>		
1 Has your organisation taken steps to minimise the use of personal data and ensure compliance with the requirements under the PDPO (e.g. using anonymised or synthetic data; understanding the sources and allowable uses of personal data; checking the accuracy of personal data, etc.)?		
2 Did your organisation take steps to ensure the reliability, integrity, accuracy, consistency, completeness, relevance, fairness and usability of data before putting it to use?		

Question	Answer (Yes/No)	Further actions required
<b>Development of AI Models</b>		
3 Did your organisation evaluate the characteristics of the machine learning algorithms before putting them to use?		
4 Did your organisation perform rigorous testing of AI models to check their reliability, robustness and fairness?		
5 Has your organisation put in place adequate risk mitigation measures, including human oversight, to deal with errors or failures that may arise in the use of the AI system?		
6 Did your organisation put in place adequate security measures to protect the AI system against attacks?		
7 Did your organisation establish contingency plans of suspending the AI system and triggering fallback solutions when it is necessary?		
<b>Management and Monitoring</b>		
8 Does your organisation keep appropriate documentation of the handling of data, risk assessments and the design, development, testing and use of the AI system?		
9 Does your organisation have any plans in place to re-assess the risks of AI when there is a significant change to the functionality or operation of the AI system, or a significant change to the regulatory or technological environment?		
10 Has your organisation reviewed, tuned and re-trained AI models periodically?		
11 Did your organisation put in place an appropriate level of human oversight for the AI system based on the assessed level of risk?		
12 Did your organisation establish operational support and feedback channels for users of the AI system?		

Question	Answer (Yes/No)	Further actions required
13 Did your organisation implement appropriate security measures throughout the AI system life cycle, from development, use, monitoring to termination?		
14 Does your organisation have any plans to conduct regular evaluation of the wider technological landscape to identify gaps in its existing technological ecosystem?		
15 Does your organisation conduct internal audit periodically to ensure compliance with internal policies in the development and use of AI?		

### COMMUNICATION AND ENGAGEMENT WITH STAKEHOLDERS

Question	Answer (Yes/No)	Further actions required
1 Did your organisation clearly and prominently disclose the use of AI to individual consumers?		
2 Did your organisation inform individual consumers of the purposes, benefits and effects of using the AI system in its products or services?		
3 Did your organisation disclose the results of risk assessment of the AI system where appropriate?		
4 Did your organisation provide channels for individuals to opt-out from using AI where possible?		
5 Were channels provided for individuals to correct any inaccuracies, provide feedback, seek explanation and request human intervention where possible?		
6 Are the communications with stakeholders made in a plain, clear and layman-understandable language?		



# PCPD's guidance

## Specifically for AI

1 Ethical Development and Use of AI (Aug 2021)

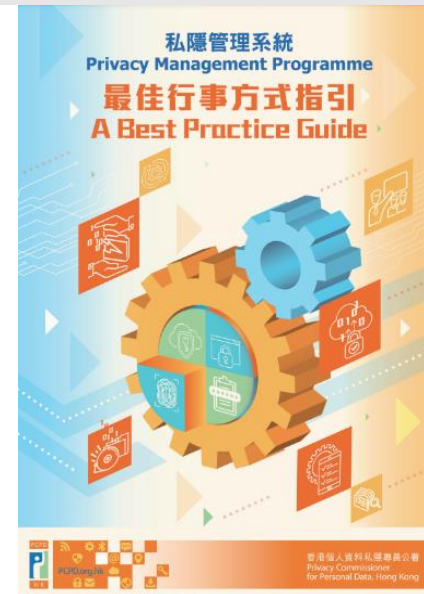


2 Tips on AI Chatbots (Sep 2023)

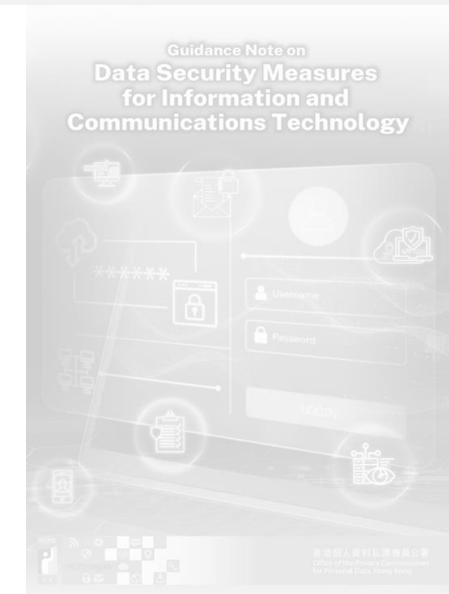


## Applicable to AI

3 Privacy Management Programme (PMP) (revised Mar 2019)



4 Data Security (Aug 2022)



# Privacy Management Programme (PMP)

## What's PMP?

- A **management framework**
  - For **responsible collection, holding, processing & use of personal data** by the company
  - To **ensure compliance with Personal Data (Privacy) Ordinance (PDPO)**

## Background

- Organisations should embrace personal data protection as part of their corporate policies and culture

## Benefits



**Minimise risk of data security incidents**



**Handle data breaches effectively** to minimize damages



**Ensure compliance** with PDPO



**Build trust** with employees and customers, enhance corporate reputation and competitiveness

**“Guide for Independent Non-Executive Directors” published by HKIoD recommends use of PMP**

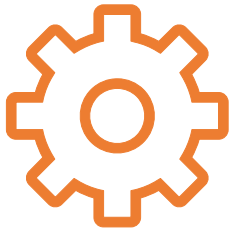


# 3 components of Privacy Management Programme (PMP)



## 1. Organisational Commitment

- Get buy-in from the top
- Appoint Data Protection Officer
- Set up a reporting mechanism



## 2. Programme Controls

- Personal data inventory
- Internal policies
- Risk assessment tools
- Training, education & promotion
- Handling of data breach incidents
- Data processor management
- Communication



## 3. Ongoing Assessment and Revision

- Develop an oversight & review plan
- Assess and revise programme controls

# PCPD's guidance

## Specifically for AI

1 Ethical Development and Use of AI (Aug 2021)



2 Tips on AI Chatbots (Sep 2023)

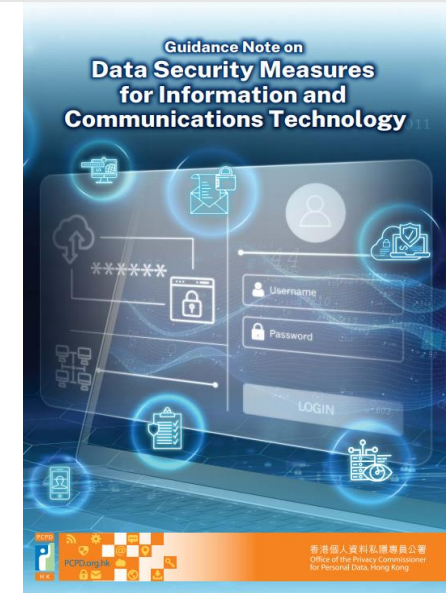


## Applicable to AI

3 Privacy Management Programme (PMP) (revised Mar 2019)



4 Data Security (Aug 2022)



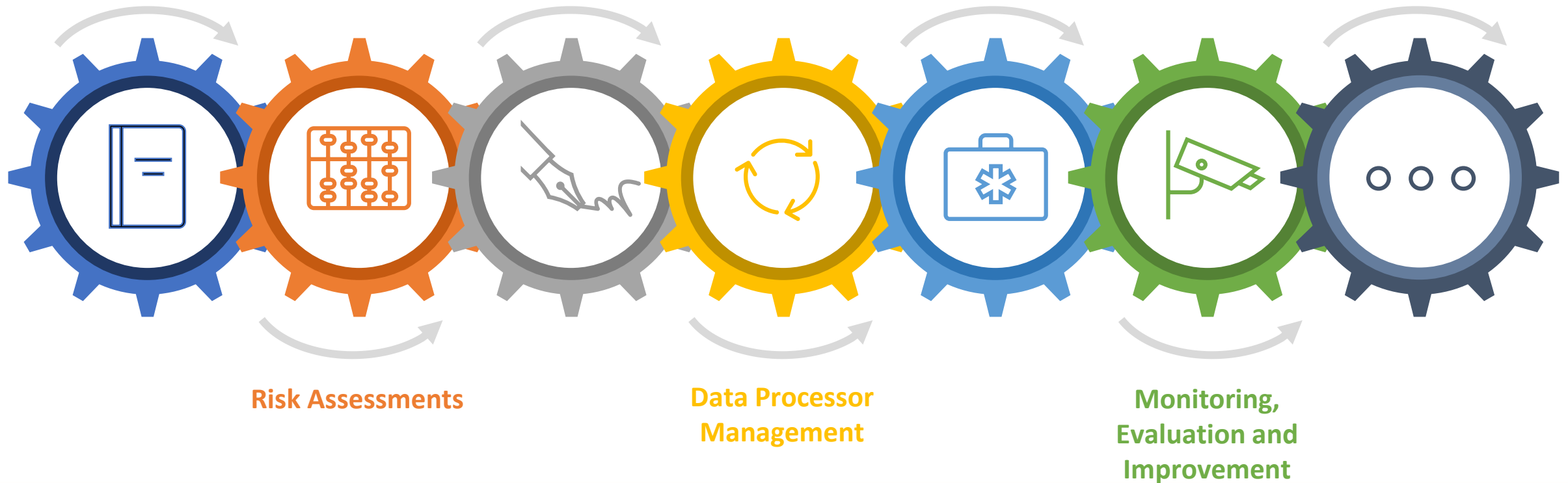
# 7 recommended measures to enhance data security

Data Governance & Organisational Measures

Technical and Operational Security Measures

Remedial Actions in the event of Data Security Accidents

Other Considerations



1

### Ethical Development and Use of AI (Aug 2021)



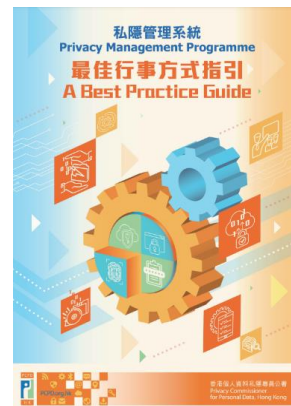
2

### 10 TIPS for Users of AI Chatbots (Sep 2023)



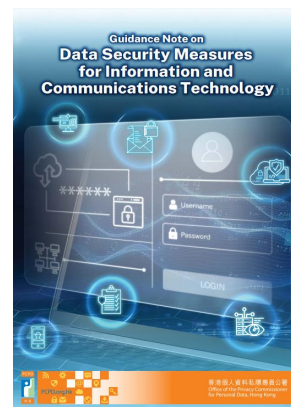
3

### Privacy Management Programme (PMP) (revised Mar 2019)



4

### Data Security Measures for Information and Communications Technology (Aug 2022)





# Thank you



2827 2827



[www.pcpd.org.hk](http://www.pcpd.org.hk)



[communications@pcpd.org.hk](mailto:communications@pcpd.org.hk)

