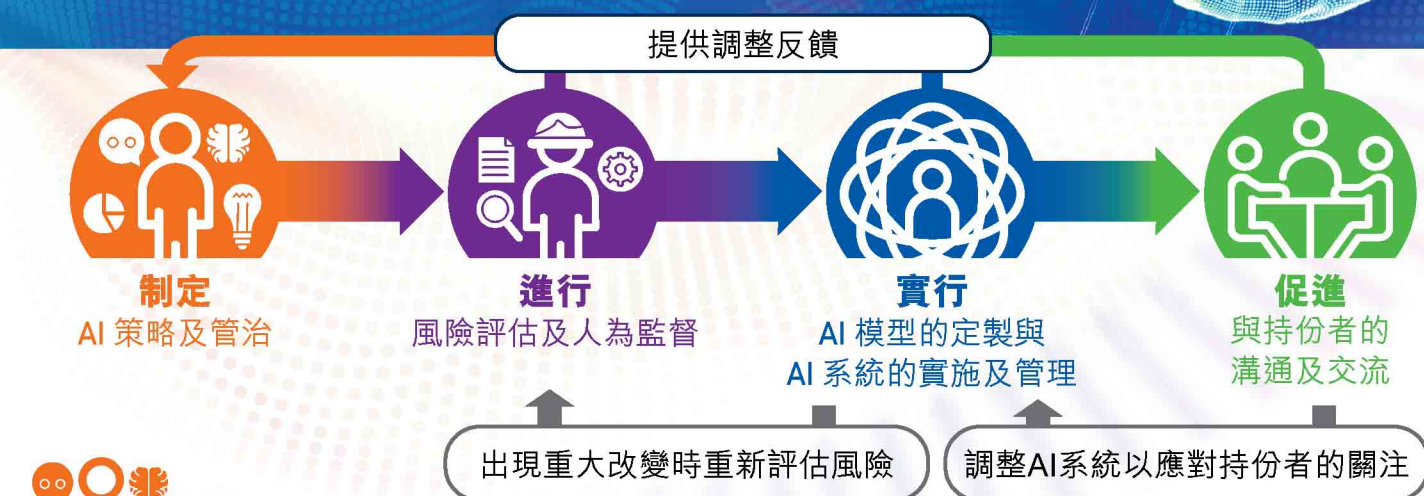


# 人工智能(AI): 個人資料保障模範框架

機構應在採購、實施及使用AI時把此框架納入業務流程



## 制定 - AI 策略及管治

### 採購 AI 7 個步驟

1. 尋找AI方案
2. 選擇合適的AI方案
3. 收集及準備數據
4. 為特定目的定製 AI 模型
5. 測試、評估和驗證AI模型
6. 測試和審核系統和組件的安全性和私隱風險
7. 將AI方案納入到機構的系統中

### 9 項管治考慮

1. 使用AI的目的
2. 私隱和保安的責任及道德規定
3. 技術性和管治方面的國際標準
4. 審查AI方案的準則及程序
5. 資料處理者協議
6. 處理AI系統生成結果的政策
7. 持續檢視環境變化的計劃
8. 監察、管理和維持AI方案的計劃
9. 評估AI供應商

支持機構：

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



## 風險為本的方式進行人為監督

較低

AI系統的風險程度

較高



**進行**  
風險評估及人為監督



**人在環外**

AI在沒有人為介入下  
作出決定



**人為管控**

人類決策者監督AI的  
運作，在有需要時介入



**人在環中**

人類決策者在決策過程中  
保留控制權



**實行**  
AI模型的定製  
與  
AI系統的實施及  
管理

### 過程

### 重點建議



確保遵從私隱法例的規定



管理數據質素



盡量減少所涉及的個人  
資料數量



妥善記錄處理數據的情況



對模型進行嚴格測試及驗證其可靠性、穩健性和公平性



在整合前，根據 AI 方案所託管的伺服器的方式（在機構  
內部或在第三方的雲端）考慮循規事宜



確保系統安全及數據安全



將記錄妥善地存檔



定期進行審核



制定AI事故應變計劃



隨著風險因素演變而考慮  
採取檢視機制



**促進**  
與持份者的溝通  
及交流

### 持份者



內部員工



AI 供應商



消費者



監管機構

PCPD



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



私隱專員公署網頁  
pcpd.org.hk

電話：2827 2827

傳真：2877 7026

地址：香港灣仔皇后大道東248號大新金融中心13樓1303室

電郵：communications@pcpd.org.hk



下載本刊物



本刊物使用署名 4.0 國際 (CC BY 4.0) 的授權條款，只要你註明原創者為香港個人資料私隱專員公署，便可自由分享或修改本刊物。  
詳情請瀏覽 [creativecommons.org/licenses/by/4.0/deed.zh\\_TW](https://creativecommons.org/licenses/by/4.0/deed.zh_TW)。

### 免責聲明

本刊物所載的資訊和建議只作一般參考用途，並非為法例的應用提供詳盡指引，亦不構成法律或其他專業意見。私隱專員並沒有就本刊物內所載的資訊和建議的準確性或個別目的或使用的適用性作出明示或隱含保證。相關資訊和建議不會影響私隱專員在《個人資料（私隱）條例》下獲賦予的職能及權力。